

Scottholme Primary and Nursery

Online Safety 2023

Scotholme Primary And Nursery School Online Safety Policy.....	0
Development / Monitoring / Review of this Policy	1
Schedule for Development / Monitoring / Review	1
Scope of the Policy.....	2
Roles and Responsibilities	3
Governors	3
Headteacher and Senior Leaders.....	3
Online Safety Coordinator.....	4
Co-ordinator for ICT.....	4
Teaching and Support Staff	5
Designated Safeguarding Leads.....	5
Online Safety Group	6
Pupils:.....	7
Parents / Carers.....	7
Community Users.....	7
Policy Statements.....	8
Education - Pupils.....	8
Education - Parents / Carers	9
Education - The Wider Community.....	9
Education & Training - Staff / Volunteers.....	10
Technical - infrastructure / equipment, filtering and monitoring	11
Mobile Technologies (including BYOD/BYOT)	12
Use of digital and video images	13
Data Protection	13
Communications.....	16
Social Media - Protecting Professional Identity	17
Dealing with unsuitable / inappropriate activities.....	18
Responding to incidents of misuse.....	20
Illegal Incidents.....	21
Other Incidents.....	22

Academy Actions & Sanctions.....	23
Appendix.....	27
Student/Pupil Acceptable Use Agreement Template - for older students/pupils.....	28
Student/Pupil Acceptable Use Policy Agreement Template - for younger pupils (Foundation/KS1)....	31
Staff (and Volunteer) Acceptable Use Policy Agreement Template.....	34
Acceptable Use Agreement for Community Users Template.....	37
Class Dojo Policy.....	38
Teams Policy	41
Responding to incidents of misuse - flow chart.....	42
Record of reviewing devices/internet sites (responding to incidents of misuse).....	43
Reporting Log.....	44
Training Needs Audit Log.....	45
Cyber Security Policy (including filtering and passwords).....	46
School/academy Personal Data Advice and Guidance.....	57
Electronic Devices - Searching & Deletion.....	70
Mobile Technologies Policy Template (inc. BYOD/BYOT).....	77
Social Media Policy.....	78
Online Safety Group Terms of Reference.....	84
Legislation.....	86
Glossary of Terms.....	94
Acknowledgements.....	95

Scottholme Primary And Nursery School
Online Safety Policy



Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group / committee (or insert name of group) made up of:

- Headteacher
- Online Safety Coordinator
- Staff - including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers
- Pupils in the school
- Community users

Consultation with the whole academy community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on:	<i>Insert date</i>
The implementation of this Online Safety policy will be monitored by the:	<i>Online Safety Coordinator</i>
Monitoring will take place at regular intervals:	<i>AT THE END OF EACH TERM</i>
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	<i>AT THE END OF EACH TERM</i>
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	<i>SEPTEMBER 2022</i>
Should serious online safety incidents take place, the following external persons / agencies should be informed:	<i>Academy Group Officials, LADO, Police</i>



The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of:
 - pupils
 - parents / carers
 - staff

Scope of the Policy

This policy applies to all members of the academy community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy digital technology systems, both in and out of the academy.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.



Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the academy:

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about online safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *Online Safety Governor*. The role of the *Online Safety Governor / Director* will include:

- annual meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings (once a year where possible)
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant *Governors / Committee / meeting*

Headteacher and Senior Leaders

- The *Headteacher and Senior Leaders* have a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the *Online Safety Coordinator*.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents - included in a later section - "Responding to incidents of misuse" and relevant *MAT* disciplinary procedures).
- The *Headteacher and Senior Leaders* are responsible for ensuring that the *Online Safety Coordinator* and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The *Headteacher* will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The *Senior Leadership Team / Senior Management Team* will receive regular termly monitoring reports from the *Online Safety Coordinator*.

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff
- liaises with the MAT
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets with Online Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of *Governors*
- reports regularly to Senior Leadership Team

Co-ordinator for ICT

The Co-ordinator for ICT is responsible for ensuring:

- that the *academy's* technical infrastructure is secure and is not open to misuse or malicious attack
- that the *academy* meets required online safety technical requirements and any MAT Online Safety Policy that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed (from the appropriate age - currently Year 4 and upwards)
- *the filtering policy (included within this policy), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the *network / internet / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher or Online Safety Coordinator* for investigation / action / sanction
- that *monitoring software / systems are implemented and updated as agreed in academy policies*

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current *academy Online Safety Policy* and practices
- they have read, understood and signed the *Staff Acceptable Use Policy (StAUP)*
- they report any suspected misuse or problem to the *Headteacher; Online Safety Coordinator* for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level *and only carried out using official school systems i.e. e-mail through the school system, the school website, Class Dojo (see Class Dojo Policy), or via Teams (see Teams Policy) using official school email addresses and logins.*
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the *Online Safety Policy* and *Pupil Acceptable Use Policies (AUP)*
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use (this should be highlighted in planning) and that processes are in place for dealing with any unsuitable material that is found in internet searches*

Designated Safeguarding Leads

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying



The Online Safety Group provides a consultative group that has wide representation from the *academy* community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the *Governing Body*.

Members of the Online Safety Group will assist the Online Safety Coordinator with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- *the production / review / monitoring of the school filtering policy and requests for filtering changes.*
- mapping and reviewing the online safety / digital literacy curricular provision - ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders - including parents / carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool



Pupils:

- are responsible for using the *academy* digital technology systems in accordance with the Pupil Acceptable Use Policy (one for KS1; one for KS2)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *academy's* Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *academy* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local online safety campaigns*. Parents and carers will be encouraged to support the *academy* in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records

Community Users

Community Users who access *academy* systems / website as part of the wider *academy* provision will be expected to sign a Community Acceptable Usage Policy before being provided with access to *academy* systems.



Education - Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in online safety / digital literacy is therefore an essential part of the academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum (see Appendix) should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and other activities
- The academy will run activities / learning related to Safer Internet Day each February.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access both on and off-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- *Pupils should be helped to understand the need for the Pupil Acceptable Use Policy and be encouraged to adopt safe and responsible use both within and outside the academy.*
- *Staff should act as good role models in their use of digital technologies, the internet and mobile devices.*
- *In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Online Safety Coordinator can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

Education - Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The academy will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, Class Dojo or the school web-sites (see <https://www.scotholme.com/online-safety.html>)*
- *Parents' / Carers' evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day, Anti-Bullying Week*
- *Reference to the relevant web-sites / publications*

Education - The Wider Community

The academy will provide opportunities for local community groups / members of the community to gain from the academy's online safety knowledge and experience. This may be offered through the following:

- *Providing family learning courses in use of new digital technologies, digital literacy and online safety*
- *Online safety messages targeted towards other relatives as well as parents.*
- *The academy website will provide online safety information for the wider community*
- *Supporting community groups where appropriate e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision*



Education & Training - Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out at least once a year.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy Online Safety Policy and Acceptable Use Policies.
- *It is expected that some staff will identify online safety as a training need within the performance management process.*
- *The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.*
- *This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.*
- *The Online Safety Coordinator will provide advice / guidance / training to individuals as required.*

Training - Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety / safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / MAT / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in academy training / information sessions for staff or parents.



Technical - infrastructure / equipment, filtering and monitoring

The academy will be responsible for ensuring that the academy infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities: **Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements.**

- **There will be regular reviews and audits of the safety and security of academy technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to academy technical systems and devices.**
- **All users from Year 4 upwards will be provided with a username and secure password by the Online Safety Coordinator who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every term**
- The "master / administrator" passwords for the academy ICT systems, used by the Network Manager (or other person) must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place (eg academy safe)*
- Online Safety Coordinator is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- **Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.**
- *The academy has provided enhanced / differentiated user-level filtering through the EMBC filters and locally through Impero software.*
- *Academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy*
- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).*
- Appropriate security measures are in place through IMS to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place, agreed with IMS for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- *An agreed policy is in place regarding the extent of personal use that users staff and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place forbids staff from downloading executable files and installing programmes on school devices, unless given permission to do so by the ICT Coordinator or if this is the staff member's school laptop. Any software installed must be from a reputable source and removed if required to do so by the ICT Coordinator or Headteacher.*
- **Staff will not use removable media to transfer data. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.**
- *Any cloud based storage will have school e-mail addresses linked to them, and any data relating to children/staff/parents will be password protected*

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the academy's wireless network. The device then has access to the wider internet which may include the academy's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the academy's Online Safety education programme.

- The school **Acceptable Use Agreements** for staff, pupils/students and parents / carers will give consideration to the use of mobile technologies
- The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device ¹	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes But locked away	Yes but used away from children except in extenuating circumstances	Yes but only used in certain areas
Full network access	Yes	Yes	Yes	No	No	No
Internet only				No	Yes	Yes as long as credentials removed afterwards

¹ Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere (e.g. Class Dojo) that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The MAT will ensure that:

- it has a Data Protection Policy.
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.

- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it.
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded.
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy' to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- it provides staff, parents, volunteers, teenagers and older children with information about how the school/academy looks after their data and what their rights are in a clear Privacy Notice
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- If a maintained school/academy, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with school/academy policy once it has been transferred or its use is complete.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted, and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with academy policy (below) once it has been transferred or its use is complete.



Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff and other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the academy	x						x	
Use of mobile phones in lessons		x						x
Use of mobile phones in social time	x							x
Taking photos on school cameras/tablets	x					x		
Use of other mobile devices to take photos				x				x
Use of personal email addresses in regard academy business				x				x
Use of academy email for personal emails		x						x
Use of messaging apps		x					x	
Use of social media				x				x
Use of blogs (associated with the school)	x					x		

When using communication technologies, the academy considers the following as good practice:

- The official *academy* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. *Staff and pupils should therefore use only the academy email service to communicate with others when in school, or on academy systems (e.g. by remote access).*
- Users must immediately report, to the nominated person (Headteacher, DSL or Online Safety Coordinator) - in accordance with the academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (e-mail, Class Dojo etc.) must be professional in tone and content. *These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Whole class / group email addresses may be used at both KS1 and KS2 where deemed appropriate*
- *Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *academy* or MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published;
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues;
- Clear reporting guidance, including responsibilities, procedures and sanctions;
- Risk assessment, including legal risk.

Academy staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or academy staff
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the *academy* or MAT;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official academy social media accounts are established, including the use of ClassDojo or Teams, there should be:

- *A process for approval or checking of communication by senior leaders;*
- *Clear processes for the administration and monitoring of these accounts - involving at least two members of staff (see ClassDojo policy)*
- *A code of behaviour for users of the accounts, including:*
 - *Systems for reporting and dealing with abuse and misuse*
 - *Understanding of how incidents may be dealt with under academy disciplinary procedures*

Personal Use:

- *Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy;*
- *Personal communications which do not refer to or impact upon the school are outside the scope of this policy;*
- *Where personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken;*
- *The academy permits reasonable and appropriate access to private social media sites.*

Monitoring of Public Social Media

- *As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school;*
- *The school should effectively respond to social media comments made by others according to a defined policy or process.*

The academy's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

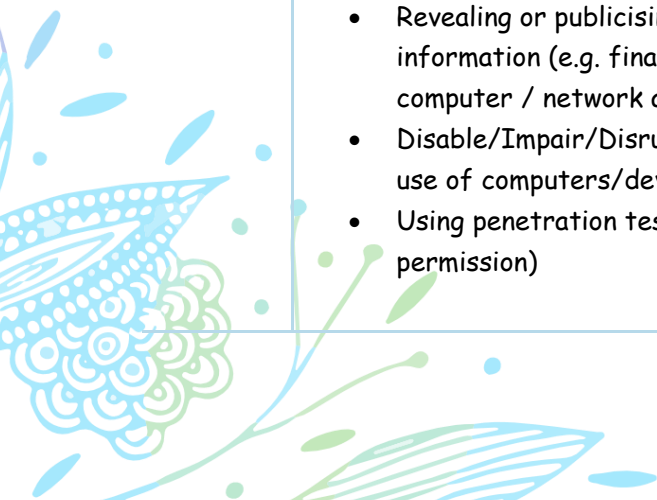
Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in an academy context, either because of the age of the users or the nature of those activities.

The academy believes that the activities referred to in the following section would be inappropriate in a academy context and that users, as defined below, should not engage in these activities in / or outside the academy when using academy equipment or systems. The academy policy restricts usage as follows:



User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images -The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK - to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
	Activities that might be classed as cyber-crime under the Computer Misuse Act: <ul style="list-style-type: none"> Gaining unauthorised access to school networks, data and files, through the use of computers/devices Creating or propagating computer viruses or other harmful files Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) Disable/Impair/Disrupt network functionality through the use of computers/devices Using penetration testing equipment (without relevant permission) 					X



User Actions	Acceptable	Acceptable at certain	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		x			
On-line gaming (non-educational)			x		
On-line gambling				x	
On-line shopping / commerce		x			
File sharing		x			
Use of social media			x		
Use of messaging apps			x		
Use of video broadcasting e.g. Youtube			x		

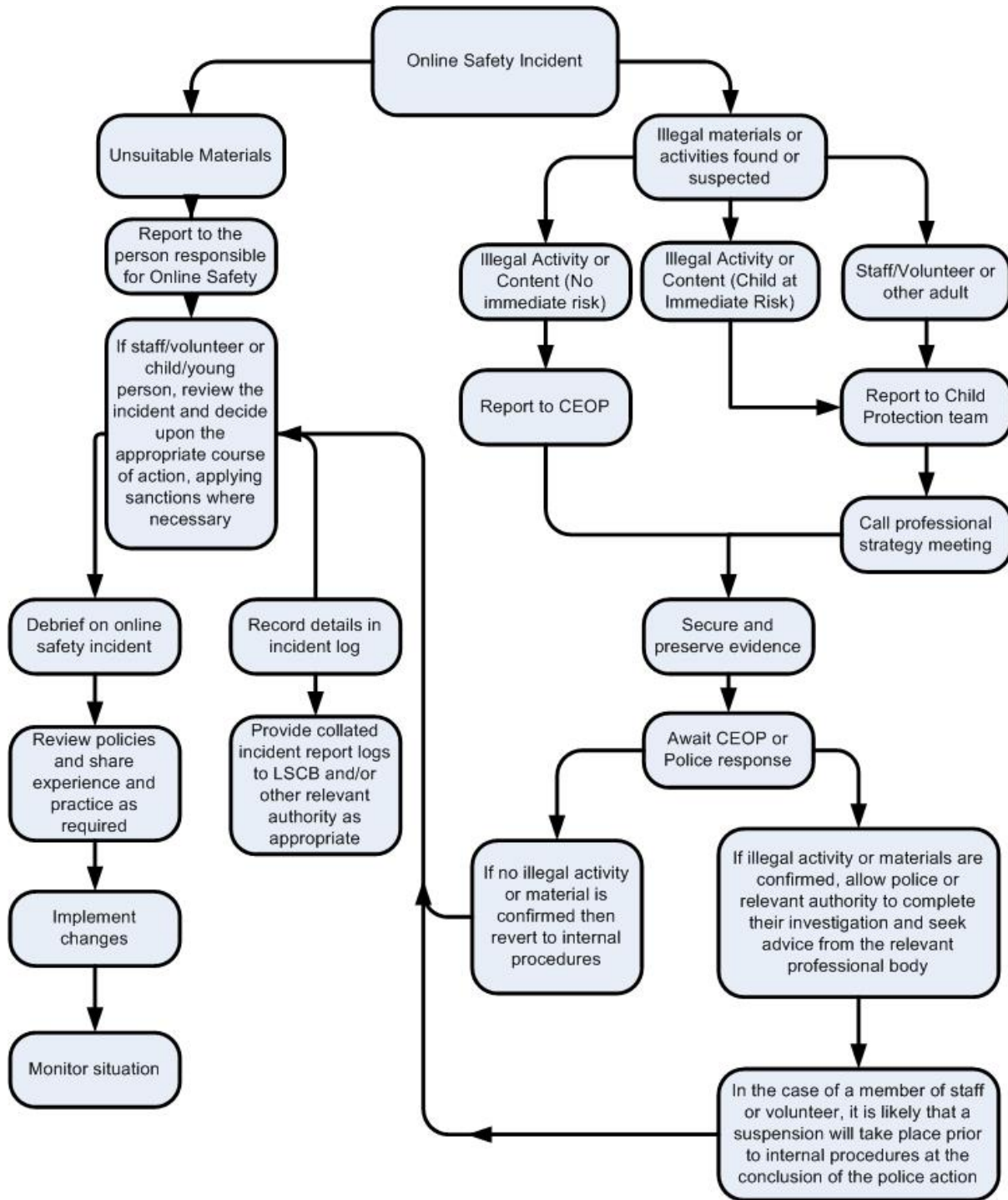
Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).



Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the academy community will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse - see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
 - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Academy Actions & Sanctions

It is more likely that the academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:



Actions / Sanctions

Pupils Incidents	Refer to class teacher / tutor	Refer to Online Safety Officer	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X		X
Unauthorised use of non-educational sites during lessons	X				X			X	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X			X	X		X	
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X			X	X		X	
Unauthorised downloading or uploading of files		X			X		X		
Allowing others to access academy network by sharing username and passwords	X	X					X	X	
Attempting to access or accessing the academy network, using another student's / pupil's account	X	X						X	
Attempting to access or accessing the academy network, using the account of a member of staff	X	X					X	X	
Corrupting or destroying the data of other users	X	X					X	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X	X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X				X	X		X

Actions which could bring the academy into disrepute or breach the integrity of the ethos of the school	x	x	x			x			
Using proxy sites or other means to subvert the academy's / academy's filtering system	x	x			x				x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x						x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x			x	x		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x			x				x



Actions / Sanctions

	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Staff Incidents								
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x				
Inappropriate personal use of the internet / social media / personal email	x							
Unauthorised downloading or uploading of files	x							
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x							
Careless use of personal data e.g. holding or transferring data in an insecure manner	x							
Deliberate actions to breach data protection or network security rules		x						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x						
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		x						
Actions which could compromise the staff member's professional standing		x						
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy		x						
Using proxy sites or other means to subvert the academy's / academy's filtering system	x							
Accidentally accessing offensive or pornographic material and failing to report the incident		x						
Deliberately accessing or trying to access offensive or pornographic material		x		x				
Breaching copyright or licensing regulations		x						
Continued infringements of the above, following previous warnings or sanctions		x						

Appendix

Appendices

Student/Pupil Acceptable Use Agreement Template - for older students/pupils.....	28
Student/Pupil Acceptable Use Policy Agreement Template - for younger pupils (Foundation/KS1)	31
Parent/Carer Acceptable Use Agreement Template.....	31
Staff (and Volunteer) Acceptable Use Policy Agreement Template	34
Acceptable Use Agreement for Community Users Template	37
Responding to incidents of misuse - flow chart.....	38
Record of reviewing devices/internet sites (responding to incidents of misuse)	43
Reporting Log.....	44
Training Needs Audit Log	45
School Technical Security Policy Template (including filtering and passwords).....	46
School/academy Personal Data Advice and Guidance.....	57
School/academy policy template: Electronic Devices - Searching & Deletion	70
Mobile Technologies Policy Template (inc. BYOD/BYOT)	77
Social Media Policy Template.....	78
School Policy Template - Online Safety Group Terms of Reference	84
Legislation.....	86
Glossary of Terms	94



Student/Pupil Acceptable Use Agreement Template - for older students/pupils

School/academy policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the *school/academy* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure - I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the *school/academy* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the *school/academy* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so. (schools/academies should amend this section to take account of their policy on each of these issues)

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school/academy*:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission (schools/academies should amend this section in the light of their mobile devices policies). I understand that, if I do use my own devices in the *school/academy*, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed (schools/academies should amend this section to take account of their policy on access to social media).

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the *school/academy* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include (schools/academies should amend this section to provide relevant sanctions as per their behaviour policies) loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student/Pupil Acceptable Use Agreement Form

This form relates to the *student/pupil* acceptable use agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems. (Schools/academies will need to decide if they require students/pupils to sign, or whether they wish to simply make them aware through education programmes/awareness raising).

I have read and understand the above and agree to follow these guidelines when:

- I use the *school/academy* systems and devices (both in and out of school)
- I use my own devices in the *school/academy* (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the *school/academy* in a way that is related to me being a member of this *school/academy* e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student/Pupil:

Group/Class:

Signed:

Date:

One document will be signed by the entire class and given to the Online Safety Coordinator to file.



Student/Pupil Acceptable Use Policy Agreement Template - for younger pupils (Foundation/KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child):

One document will be signed by the entire class and given to the Online Safety Coordinator to file.



Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. *Students/Pupils* and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's **delete as relevant** first name/initials will be used.

The school will comply with the Data Protection Act and request parent's/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

As the school/academy is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)	The images
Who will have access to this form.	Where the images may be published. Such as; Twitter, Facebook, the school/academy website, local press, etc. (see relevant section of form below)
Where this form will be stored.	Who will have access to the images.
How long this form will be stored for.	Where the images will be stored.
How this form will be destroyed.	How long the images will be stored for.
	How the images will be destroyed.

	How a request for deletion of the images can be made.
--	---

Digital/Video Images Permission Form

Parent/Carers Name: Student/Pupil Name:

As the parent/carer of the above student/pupil, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
<ul style="list-style-type: none"> to support learning activities. 	Yes/No
<ul style="list-style-type: none"> in publicity that reasonably celebrates success and promotes the work of the school. 	Yes/No
Insert statements here that explicitly detail where images are published by the school/academy	Yes/No
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes/No

Signed:

Date:



Staff (and Volunteer) Acceptable Use Policy Agreement Template

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school/academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students/pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that *students/pupils* receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *academy* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school/academy* systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems such as Class Dojo or Teams. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school/academy*:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using *school/academy* equipment. I will also follow any additional rules set by the *school/academy* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the *school/academy* ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant *school/academy* policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in *school/academy* policies unless given permission by the Online Safety Lead
- I will not disable or cause any damage to *school/academy* equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by *school/academy* policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school/academy*:

- I understand that this acceptable use policy applies not only to my work and use of school/academy digital technology equipment in school, but also applies to my use of school/academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school/academy
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to *Governors/directors* and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:



Acceptable Use Agreement for Community Users Template

This acceptable use agreement is intended to ensure:

- that community users of school/academy digital technologies will be responsible users and stay safe while using these systems and devices
- that school/academy systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school/academy:

- I understand that my use of school/academy systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school/academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school/academy has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: Signed: Date:

Class Dojo Policy

What is Class Dojo?

Scotholme Primary School uses Class Dojo to communicate with parents and keep them informed about what is happening in school. We have used it through school closures during the pandemic and continue to use it to communicate with staff and provide online work for the pupils at Scottholme Primary School.

Class Dojo has the ability to create a Class Story, which is a record of what the class have been doing in school or on visits. Each child then has a separate Story, which can be used to show parents what their child has been doing.

Within the app, it is possible to directly message parents, meaning that the school can remind parents about bringing PE kits, special events or visits out of school. Parents can also send messages to the class teacher, giving notice about absence or issues that have arisen at home.

Home Learning

Lessons for English, Maths and Foundation subjects will be posted on Dojo each day in PDF format.

Links to YouTube videos to assist with these lessons will be posted alongside these.

Activities can be set in the Portfolio for the children to respond electronically if the child is capable of doing so. Teachers can respond with feedback through Portfolio.

Homework will be sent through the app during normal school opening times, making sure that parents know that homework has been set.

Finally, Class Dojo will also record the school's reward system of House Points. Each child can be awarded points for a number of different reasons, all adding to their total, no matter which teacher awards the points to them.

Policy

- Each class will use ClassDojo through their whiteboard (via a web browser) or on the Class iPad.
- Each teacher will have an account and be connected with the school via their Scottholme e-mail address.
- Staff will need to lock their computers and iPad upon leaving the computer so that nobody can access their account.

Communications

- Staff will communicate with parents in a professional manner at all times.

- **No negative messages should be sent via Dojo - parents should be telephoned or asked to come into school for a meeting if necessary.**
- **Staff should check their communications before sending to parents to make sure that:**
 - **There are no spelling or grammatical errors;**
 - **The communication makes sense and cannot be mis-interpreted;**
 - **The communication is being sent to the correct person/people.**
- **Staff are not required to answer messages at all times and may set 'Do Not Disturb' periods. In fact, the school recommends that the staff do not answer any messages before 8am or after 6pm to maintain a work/life balance.**
- **Staff should not enter into dialogue with parents in the event that they are unhappy about something - they should ask the parent to organise a meeting with them as soon as is appropriate.**
- **If parents are not connected to Dojo, staff should send a reminder or ask the staff in the office to chase up registration.**
- **New entrants will be signed up for Class Dojo when they are filling in the admission form, so that they can immediately receive communications.**

School Story

- **Staff should be aware that this Story will be visible by all parents and teachers.**
 - **Staff should check spellings, grammar and that any dates are correct before posting;**
 - **Events which effect the whole school should be posted here. Any children who don't have permission to be on the school website should not be photographed;**
 - **Individual children should not be photographed and placed on this section;**
 - **When posting to this section, children in the photographs should not be named;**
 - **If children are named in a post, only their first names should be used.**

Class and Individual Stories

- **Class Stories**
 - **Staff need to be aware that anything published on this part of Dojo can be seen by all the parents of the children in that class;**
 - **All of the factors from the School Story should be considered here too.**
- **Individual Stories**
 - **Only the child who is the subject of the story should be photographed in this section - no other children should be visible.**
 - **Photographs which do not allow a child to be identified e.g. the back of their head etc are acceptable.**
 - **Only positive comments should be posted.**
 - **Staff should discuss with children what they should post to this section.**

Child Portfolios

- **When children have created accounts, they can post photos and comments to their own Portfolio and complete work that has been set by their teacher.**

- Children need to understand what is appropriate to post here and that it is not a forum to have conversations with their teacher.
- Teachers should only use this to give feedback on work.

Comments/Likes

It is possible for parents and children to 'Like' posts or make comments on posts. Staff should monitor these (they will receive notifications that children or parents have done this), so that inappropriate comments can be removed.

Staff can then help children (or parents) understand what is appropriate in a comment. This will support the Online Safety work done in school.



Teams Policy

Teams

All Teams in school must have more than 1 adult in them and ideally have a member of the Leadership team assigned to it.

All Meetings must be done through Teams and no other platform.

All Teams Meetings should have always more than 1 adult from school.

There should be no 1-to-1 Meetings.

Meetings

When setting up lessons, make sure that the children are set as Attendees.

Set up the Meeting so that nobody can bypass the lobby and only the teachers can present.

Initially, don't 'Allow attendees to unmute'. You can change this during the Meeting once everything is settled.

Think carefully about where you are presenting from, ensuring that there is nothing inappropriate or distracting in the background. Consider masking your background if presenting from home.

Decide whether you want the children to have their cameras on or off. It is usual to have the cameras on to begin with so that they can see each other but then turn them off so that they are not distracted by each other.

Don't allow 1 child into the Meeting from the lobby. Always make sure that you have the other adult present first. Ideally, you will admit several children at once from the lobby.

Ensure you know how to:

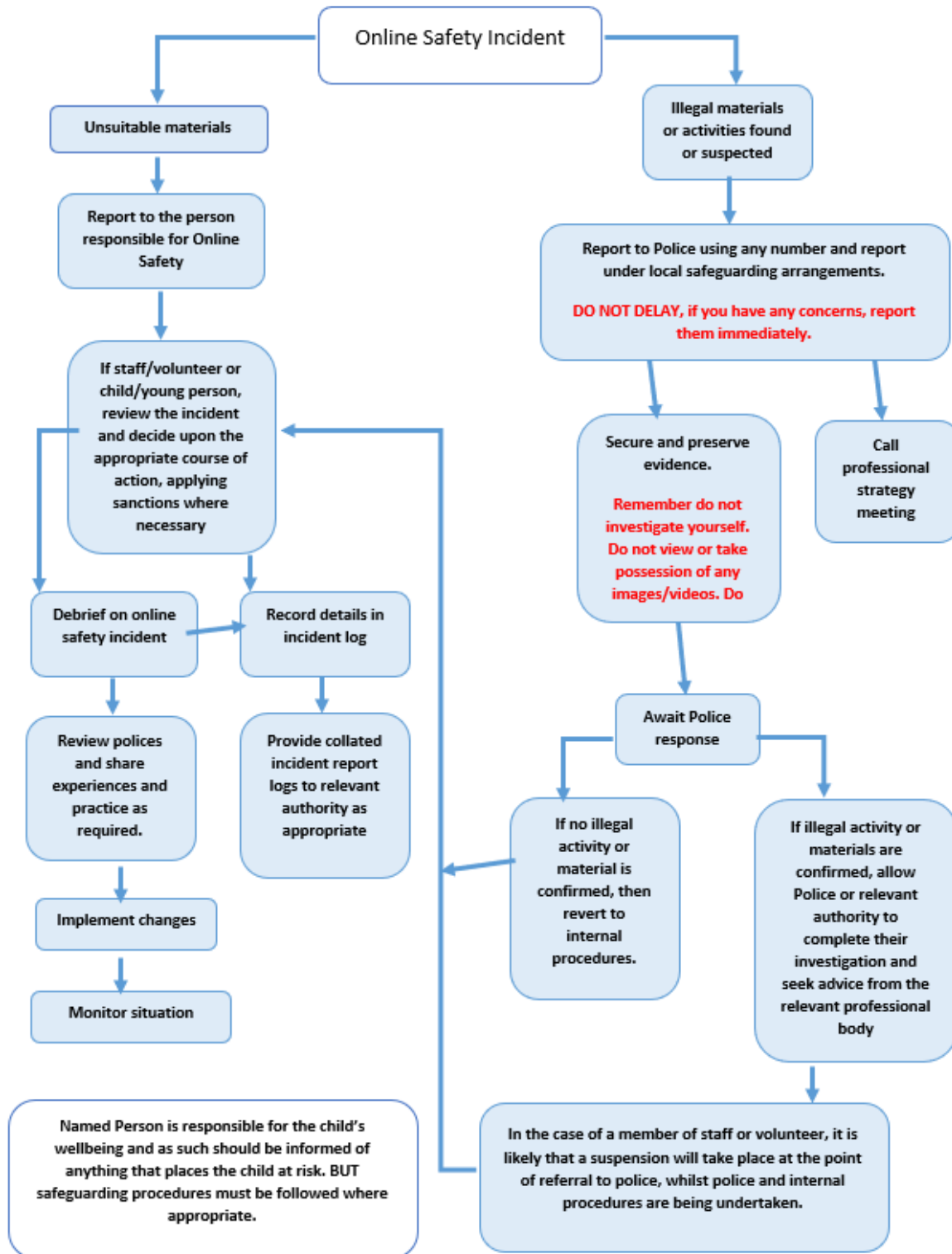
- mute all participants;
- remove people from the meeting (if necessary);
- can 'Spotlight' yourself (and 'un-Spotlight' yourself).

If sharing your screen, think carefully about windows that may be open on your computer so that sensitive information cannot be seen (GDPR still applies).

Setting work

Make sure that this is appropriate to the children's age and stage - will they manage to do work via Teams or is it better to just use Teams for visual contact?

Responding to incidents of misuse - flow chart



Record of reviewing devices/internet sites (responding to incidents of misuse)

Group:

Date:

Reason for investigation:

.....

.....

Details of first reviewing person

Name:

Position:

Signature:

Details of second reviewing person

Name:

Position:

Signature:

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken





the online safety self-review tool

Reporting Log

Group:

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		



the online safety self-review tool

Training Needs Audit Log

Group:

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

Cyber Security Policy (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure/network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.



1.1 Cyber security has been identified as a risk for the School and every employee needs to contribute to ensure data security.

1.2 The School has invested in technical cyber security measures, but we also need our employees to be vigilant and act to protect the School IT systems.

1.4 The Headteacher is responsible for cyber security within the School.

1.5 If you are an employee, you may be liable to disciplinary action if you breach this policy.

1.6 This policy supplements other data management and security policies.

2. Purpose and scope

2.1 The purpose of this document is to establish systems and controls to protect the School from cyber criminals and associated cyber security risks, as well as set out an action plan should the School fall victim to cyber-crime.

2.2 This policy is relevant to all staff.

3. What is cyber-crime?

3.1 Cyber-crime is simply a crime that has some kind of computer or cyber aspect to it. It takes shape in a variety of different forms, e.g. hacking, phishing, malware, viruses or ransom attacks.

3.2 The following are all potential consequences of cyber-crime which could affect individuals and/or individuals: -

□ cost;

□ confidentiality and data protection;

□ potential for regulatory breach;

□ reputational damage;

□ business interruption; and

□ structural and financial instability.

3.3 It is important, given the serious consequences above, to be careful not to be the victim of cyber-crime and to follow the guidance within this policy.

4. Cyber-crime prevention

4.1. This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime. The Headteacher can provide further details of other aspects of the school/Trust risk assessment process upon request.

4.2. The School have put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance to staff.

4.3 Technology solutions

(a) The School have a variety of technical measures in place for protection against cyber-crime. They include:

- (i) firewalls;
- (ii) anti-virus software;
- (iii) anti-spam software;
- (iv) auto or real-time updates on our systems and applications;
- (v) URL filtering;
- (vi) secure data backup;
- (vii) encryption and cloud storage through Microsoft 365;
- (viii) deleting or disabling unused/unnecessary user accounts;
- (ix) deleting or disabling unused/unnecessary software;
- (x) using strong passwords; and
- (xi) disabling auto-run features.

4.4. Controls and guidance for staff

(a) all staff must follow the policies related to cyber-crime and cyber security as listed in the introduction to this policy.

(b) all staff will be provided with training at induction and refresher training as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the School or any third parties with whom we share data.

(c) all staff must:

- (i) choose strong passwords;
- (ii) keep passwords secret;
- (iii) never reuse a password;
- (iv) never allow any other person to access the school's systems using your login details;

(v) not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on their computer, phone or network or the School IT systems;

(vi) report any security breach, suspicious activity, or mistake made that may cause a cyber security breach, to the Head teacher or Online Safety Coordinator as soon as practicable from the time of the discovery or occurrence.

(vii) only access work systems using computers that or devices that are not machines available to the public..

(viii) do not install software onto your School computer without consulting the Online Safety Coordinator or Schools IT.

(ix) avoid clicking on links to unknown websites, downloading large files, or accessing inappropriate content using School equipment or networks.

(d) all staff must not misuse IT systems. The School considers the following actions to be a misuse of its IT systems or resources:

(i) any malicious or illegal action carried out against the School or using the School's systems;

(ii) accessing inappropriate, adult or illegal content within School premises or using School equipment;

(iii) excessive personal use of School's IT systems during working hours;

(iv) removing data or equipment from School premises or systems without permission, or in circumstances prohibited by this policy;

(v) using School equipment in a way prohibited by this policy;

(vi) circumventing technical cyber security measures implemented by the School's IT team; and

(vii) failing to report a mistake or cyber security breach.

5. Cyber-crime incident management plan

5.1. The incident management plan consists of four main stages:

(i) Containment and recovery to include investigating the breach and utilising appropriate staff to mitigate damage and recover any data lost where possible.

(ii) Assessment of the ongoing risk to include confirming what data has been affected, what happened, whether relevant data was protected and how sensitive it is and identifying any other consequences of the breach/attack.

(iii) Notification to consider if the cyber-attack needs to be reported to regulators (for example the ICO) and/or colleagues/parents as appropriate.

(iv) Evaluation and response to consider any improvements to data security and evaluate future threats to security.

5.2 Where it is apparent that a cyber security incident involves a personal data breach, the school will invoke their Data Breach Policy.

The management of technical security will be the responsibility of the Online Safety Coordinator in conjunction with Schools IT.

Technical Security

Policy statements

The school/academy will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- school technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling must be securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work-stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school/academy systems and data
- responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- all users will have clearly defined access rights to school/academy technical systems.
- users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The IT Coordinator and Schools IT are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- *mobile device security and management procedures are in place using Meraki and Netsweeper*
- *academy and technical staff regularly monitor and record the activity of users on the school/academy technical systems and users are made aware of this in the acceptable use agreement.*
- *remote management tools are used by staff to control workstations and view users activity*

- *an appropriate system is in place for users to report any actual/potential technical incident to the online safety co-ordinator/network manager/technician (or other relevant person, as agreed)*
- an agreed policy is in place for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school/academy system.
- *an agreed policy is in place where the Online Safety Coordinator or SchoolsIT decide regarding the downloading of executable files and the installation of programmes on school/academy devices by users*
- *an agreed policy is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school/academy devices that may be used out of school*
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school/academy devices
- the school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- personal data cannot be sent over the internet or taken off the school/academy site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all school/academy technical systems, including networks, devices, email and learning platform). You can find out more about passwords, why they are important and how to manage them in our blog article. You may wish to share this with staff members to help explain the significance of passwords as this is helpful in explaining why they are necessary and important. Two factor authentication is encouraged on any mobile devices used when accessing sensitive, personal data.

Policy Statements:

- These statements apply to all users.
- All school/academy networks and systems will be protected by secure passwords.
- All users have clearly defined access rights to school/academy technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the online safety group (or other group).
- All users (adults and students/pupils) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by SchoolsIT, the academy business manager or the Online Safety Coordinator who will keep an up to date record of users and their usernames.



Password requirements:

- Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school/academy
- Passwords must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on first login to the system

Learner passwords:

- Records of learner usernames and passwords for foundation phase students/pupils can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. *Password complexity in foundation phase should be reduced (for example 6-character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.*
- Password requirements for students/pupils at Key Stage 2 and above should increase as students'/pupils progress through school/academy.
- Users will be required to change their password if it is compromised.
- Students/pupils will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.
- Pupils who require their passwords to be reset will need to ask their teacher who will then ask the Online Safety Coordinator to reset.

Notes for technical staff/teams

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration should also be given to using two factor authentication for such accounts.
- An administrator account password for the school/academy systems should also be kept in a secure place e.g. school/academy safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.
- Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.
- *It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.*
- *Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by SchoolsIT, the academy business manager or the Online Safety Coordinator. Good practice is that the password generated*

by this change process should be system generated and only known to the user. This password should be temporary and the user should be forced to change their password on first login. The generated passwords should also be long and random.

- *Where automatically generated passwords are not possible, then a good password generator should be used by by SchoolsIT, the academy business manager or the Online Safety Coordinator.) to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary and the user should be forced to change their password on the first login.*
- *Requests for password changes should be authenticated by Online Safety Coordinator to ensure that the new password can only be passed to the genuine user*
- *Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use. (For example, your technical team may provide pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system after use.)*
- *Passwords shall not be displayed on screen, and shall be securely hashed when stored (use of one-way encryption).*

Training/Awareness:

Members of staff will be made aware of the school/academy's password policy:

- at induction
- through the school/academy's online safety policy and password security policy
- through the acceptable use agreement

Students/pupils will be made aware of the school's/college's password policy:

- in lessons
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:

The responsible person, the Online Safety Coordinator will ensure that full records are kept of:

- User Ids and requests for password changes
- *User logons*
- *Security incidents related to this policy*

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by by SchoolsIT, the academy business manager or the Online Safety Coordinator.. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- **be logged in change control logs**
- **be reported to a second responsible person** (any of the three DSLs)
-

All users have a responsibility to report immediately to (insert title) any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- Either - The school/academy maintains and supports the managed filtering service provided by the Internet Service Provider (or other filtering service provider)
- Or - The school/academy manages its own filtering service
- The school has provided enhanced/differentiated user-level filtering through the use of the (insert name) filtering programme. (allowing different filtering levels for different ages/stages and different groups of users - staff/pupils/students etc.)
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher/Principal (or other nominated senior leader).
- Mobile devices that access the school/academy internet connection (whether school/academy or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff (insert name or title) (N.B. an additional person should be nominated -

to ensure protection for the Network Manager or any other member of staff, should any issues arise re unfiltered access). If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

Education/Training/Awareness

Pupils/students will be made aware of the importance of filtering systems through the online safety education programme (schools may wish to add details). They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through: (amend as relevant)

- the acceptable use agreement
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc. (amend as relevant)

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to their teacher who will then pass information on to the Online Safety Coordinator who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the school online safety policy and the acceptable use agreement. *Monitoring will take place as follows: once a term, the Online Safety Coordinator will check the logs and look for patterns or unusual activity.*

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to: (schools should amend as relevant)

- the second responsible person (insert title)
- Online Safety Group
- Online Safety Governor/Governors committee
- External Filtering provider/Local Authority/Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites - in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents

where users try to subvert the filtering system might suggest that improved monitoring/disciplinary action might be necessary).

Further Guidance

Schools/academies may wish to seek further guidance. The following is recommended:

Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" (Revised Prevent Duty Guidance: for England and Wales, 2015).

The Department for Education 'Keeping Children Safe in Education' requires schools to: "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

In response UKSIC produced guidance on - information on "Appropriate Filtering"

Somerset Guidance for schools - questions for technical support - this checklist is particularly useful where a school/academy uses external providers for its technical support/security.

SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed: SWGfL Test Filtering



School/academy Personal Data Advice and Guidance

Please see [Shine MAT GDPR Policies](#)

Suggestions for use

Data Protection Law - A Legislative Context

With effect from 25th May 2018, the data protection arrangements for the UK changed following the implementation of the European Union General Data Protection Regulation (GDPR). This represented a significant shift in legislation and in conjunction with the Data Protection Act 2018 replaced the Data Protection Act 1998.

GDPR - As a European Regulation, the GDPR has direct effect in UK law and automatically applies in the UK until we leave the EU (or until the end of any agreed transition period, if we leave with a deal). After this date, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

Data Protection Act 2018 - this Act sits alongside the GDPR, and tailors how the GDPR applies in the UK and provides the UK-specific details such as: how to handle education and safeguarding information.

No Deal Brexit -The Information Commissioner advises that in the event of a no- deal Brexit it is anticipated that the Government of the day will pass legislation to incorporate GDPR into UK law alongside the DPA 2018. Unless your school/academy receives personal data from contacts in the EU there will be little change save to update references to the effective legislation in privacy notices etc.

In this document the term "Data Protection Law" refers to the legislation applicable to data protection and privacy as applicable in the UK from time to time.

Does the Data Protection Law apply to schools?

In short, yes. Any natural or legal person, public authority, agency or other body which processes personal data is considered a 'data controller'.

A school/academy is, for the purposes of the Data Protection Law, a "public body" and further processes the **personal data** of numerous **data subjects** on a daily basis.

Personal data is information that relates to an identified or identifiable living individual (a data subject).

Guidance for schools/academies is available on the [Information Commissioner's Office \(ICO\)](#) website including information about the Data Protection Law.

The ICO's powers are wide ranging in the event of non-compliance and schools/academies must be aware of the huge impact that a fine or investigation will have on finances and also in the wider community for example in terms of trust.

The Data Protection Law sets out that a data controller must ensure that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to data subjects;
- b) collected for specified, explicit and legitimate purposes and not further processed in a

- manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Data Protection Law in order to safeguard the rights and freedoms of data subjects; and
 - f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These principles of the Data Protection Law drive the need for the school/academy to put in place appropriate **privacy notices** (to give a data subject information about the personal data processing activities, **legal basis of processing** and **data subject rights**) and policies (such as for reporting a breach, managing a data subject access request, training, retention etc.) to demonstrate compliance.

Data Mapping to identify personal data, data subjects and processing activities

The school/academy and its employees will collect and/ or process a wide range of information concerning numerous data subjects and some of this information will include personal data. Further, the school/academy may need to share some personal data with third parties. To be able to demonstrate and plan compliance and it is important that the school/academy has a **data map** of these activities; it can then make sure that the correct privacy notices are provided, put in place **security measures** to keep the personal data secure and other steps to avoid **breach** and also put in place data processing agreements with the third parties.

The data map should identify what personal data held in digital format or on paper records in a school/ academy, where it is stored, why it is processed and how long it is retained.

In a typical data map for a school/academy the data subjects and personal data will include, but is not limited to:

- Parents, legal guardians, governors - and personal data of names, addresses, contact details

- Learners - curricular / academic data e.g. class lists, learner progress records, reports, references, contact details, health and SEN reports
- Staff and contractors - professional records e.g. employment history, taxation and national insurance records, appraisal records and references, health records

Some types of personal data are designated as '**special category**' being personal data; "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

This should be identified separately and to lawfully process special category data, you must identify both a lawful basis and a separate condition for processing special category data. You should decide and document this before you start processing the data.

The school/academy will need to identify appropriate lawful process criteria for each type of personal data and if this is not possible such activities should be discontinued. The lawful processing criteria can be summarised as:

- | | |
|---------------------------|---|
| (a) Consent: | the data subject has given clear consent for you to process their personal data for a specific purpose (see below for further guidance) |
| (b) Contract: | the processing is necessary for a contract you have with the data subject |
| (c) Legal obligation: | the processing is necessary for you to comply with the law (not including contractual obligations). |
| (d) Vital interests: | the processing is necessary to protect someone's life. |
| (e) Public task: | the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. |
| (f) Legitimate interests: | the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks) Please also be aware that these criteria must be supported by a written legitimate interest assessment. |

No single basis is 'better' or more important than the others - which basis is most appropriate to use will depend on your purpose and relationship with the data subject.

Several of the lawful purpose criteria may relate to a particular specified purpose - a legal obligation, a contract with the individual, protecting someone's vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.

As a public authority, and if you can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the public task basis. If not, you may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and your relationship with the data subject. There is no absolute ban on public authorities using consent or legitimate interests as their lawful basis, but the Data Protection law does restrict public authorities' use of these two criteria.

The majority of processing of personal data conducted by public authorities will fall within Article 6(1)(e) GDPR, that "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*" however careful consideration must be given to any processing, especially in more novel areas. As you can see, consent is just one of several possible lawful processing criteria.

Consent has changed as a result of the GDPR and is now defined as: "in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data"

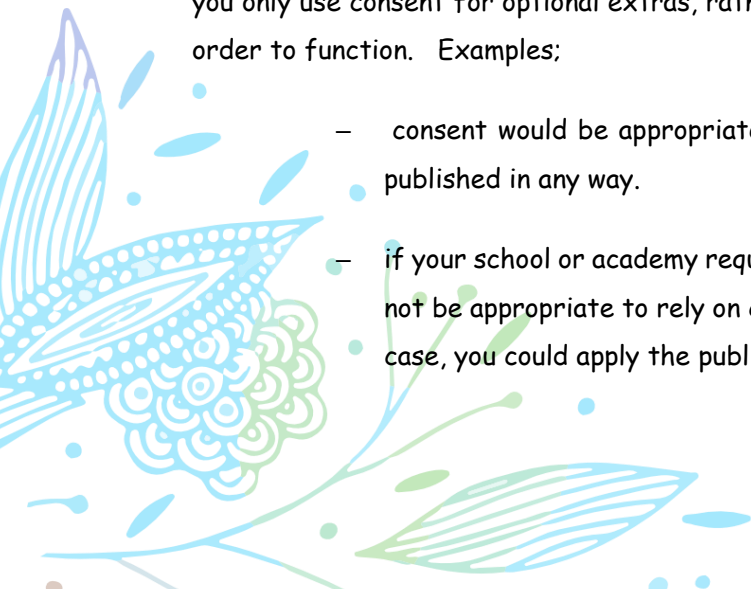
This means that where a school/academy is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. The GDPR does not specify an age of consent for general processing but schools/academies should consider the capacity of pupils to freely give their informed consent.

The Information Commissioner's Office (ICO) gives clear advice on when it's appropriate to use consent as a lawful base. It states:

"Consent is appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair."

You should only use consent if none of the other lawful bases is appropriate. If you do so, you must be able to cope with people saying no (and/or changing their minds), so it's important that you only use consent for optional extras, rather than for core information the school requires in order to function. Examples;

- consent would be appropriate for considering whether a child's photo could be published in any way.
- if your school or academy requires learner details to be stored in an MIS, it would not be appropriate to rely on consent if the learner cannot opt out of this. In this case, you could apply the public task lawful base.



Content of Privacy Notices

Privacy Notices are a key compliance requirement as they ensure that each data subject is aware of the following points when data is collected/ processed by a data controller:

- Who the controller of the personal data is
- What personal data is being processed and the lawful purpose of this processing
- where and how the personal data was sourced
- to whom the personal data may be disclosed
- how long the personal data may be retained
- data subject's rights and how to exercise them or make a complaint

In order to comply with the fair processing requirements in data protection law, the school/academy will inform parents/carers of all learners of the data they collect, process and hold on the learners, the purposes for which the data is held and the third parties (e.g. LA etc.) to whom it may be passed. This privacy notice will be passed to parents/carers for example in the prospectus, newsletters, reports or a specific letter / communication or you could publish it on your website and keep it updated there. Parents/carers of young people who are new to the school/academy will be provided with the privacy notice through an appropriate mechanism.

In some circumstances you may also require privacy notices for children / learners as data subjects as children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased. The policies that explain this should be clear and age appropriate.

Data subject's right of access

Data subjects have a number of rights in connection with their personal data. They have the right:

- to be informed - Privacy Notices
- of access - Subject Access Requests
- to rectification - correcting errors
- to erasure - deletion of data when there is no compelling reason to keep it
- to restrict processing - blocking or suppression of processing
- to portability - unlikely to be used in a school/academy context
- to object - objection based on grounds pertaining to their situation
- related to automated decision making, including profiling

Several of these could impact schools and academies, such as the right of access. You need to put procedures in place to deal with Subject Access Requests. These are written or verbal requests to see all or a part of the personal data held by the Controller in connection with the data subject. Controllers normally have 1 calendar month to provide the information, unless the case is unusually complex in which case an extension can be obtained.

A school/academy must not disclose personal data even if requested in a Subject Access Request;

- if doing so would cause serious harm to the individual
- child abuse data
- adoption records
- statements of special educational needs

Your school or academy must provide the information free of charge. However, if the request is clearly unfounded or excessive - and especially if this is a repeat request - you may charge a reasonable fee.

Breaches and how to manage a breach

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high profile issue for schools, academies and other organisations. It is important that the school/academy has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- no school/academy or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, put individuals at risk and affect personal, professional or organisational reputation
- schools/academies are "data rich" and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- the school/academy will want to avoid the criticism and negative publicity that could be generated by any-personal data breach

Schools / academies have always held personal data on the learners in their care, and increasingly this data is held digitally and accessible not just in school/academy but also from remote locations.

It is important to stress that the Data Protection Laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

Schools / Academies will need to carefully review their policy, in the light of pertinent Local Authority regulations and guidance and changes in legislation.

All significant data protection incidents must be reported through the DPO to the Information Commissioner's Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.

If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. You do not need to report every breach to the ICO.

The school/academy should have a policy for reporting, logging, managing and recovering from information risk incidents, which establishes a:

- "responsible person" for each incident
- communications plan, including escalation procedure
- plan of action for rapid resolution
- plan of action of non-recurrence and further awareness raising

Privacy by Design and Data Protection Impact Assessments (DPIA)

Data Protection Impact Assessments (DPIA) identify and address privacy risks early on in any project so that you can mitigate them before the project goes live.

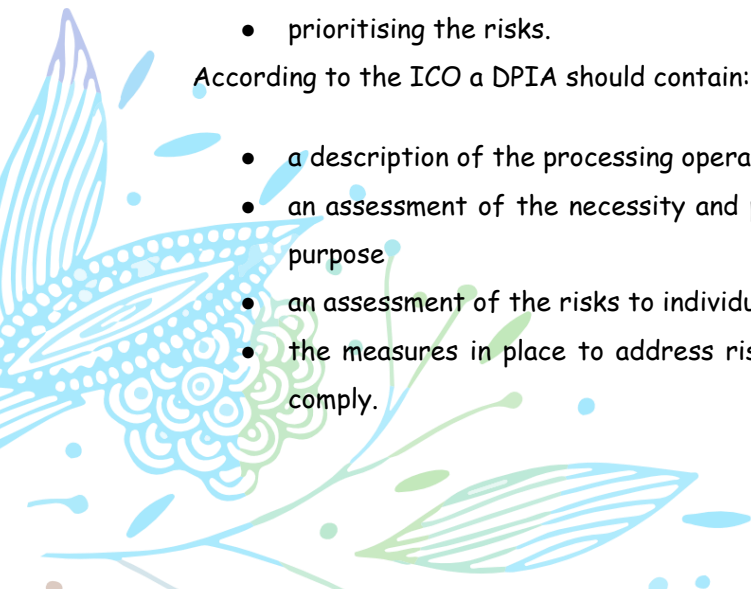
DPIAs should be carried out by Data Managers (where relevant) under the support and guidance of the DPO. Ideally you should conduct a DPIA before processing activity starts. However, some may need to be retrospective in the early stages of compliance activity.

The risk assessment will involve:

- recognising the risks that are present
- judging the level of the risks (both the likelihood and consequences)
- prioritising the risks.

According to the ICO a DPIA should contain:

- a description of the processing operations and the purpose
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an assessment of the risks to individuals
- the measures in place to address risk, including security and to demonstrate that you comply.



Or more simply and fully:

- who did you talk to about this?
- what is going to happen with the data and how - collection, storage, usage, disposal
- how much personal data will be handled (number of subjects)
- why you need use personal data in this way
- what personal data (including if it's in a 'special category') are you using
- at what points could the data become vulnerable to a breach (loss, stolen, malicious)
- what the risks are to the rights of the individuals if the data was breached
- what are you going to do in order to reduce the risks of data loss and prove you are compliant with the law.

DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started.

Secure storage of and access to data

The school/academy should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Good practice suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school/academy equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school/academy personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software

- The data must be securely deleted from the device, in line with school/academy policy once it has been transferred or its use is complete.

The school/academy will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

The school/academy should have a clear policy and procedures for the automatic backing up, accessing and restoring of all data held on school/academy systems, including off-site backups.

The school/academy should have clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Microsoft 365, Google Drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school/academy will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

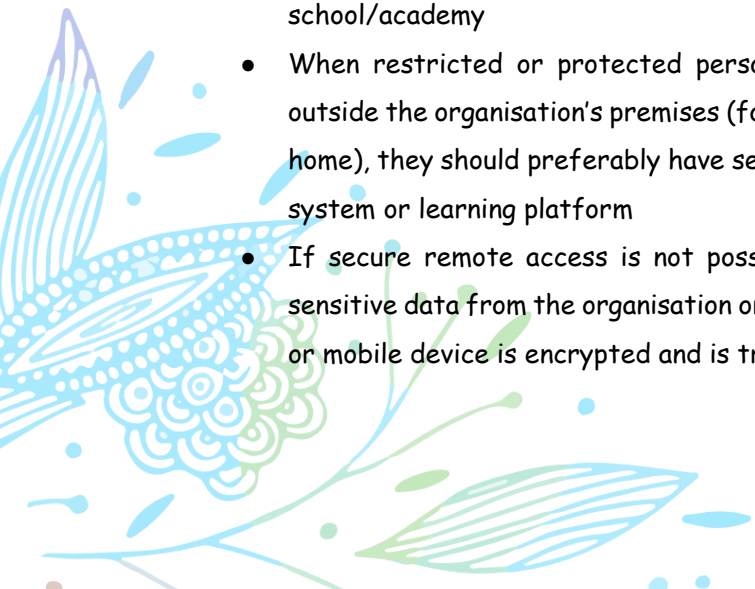
As a Data Controller, the school/academy is responsible for the security of any data passed to a "third party". Specific data processing clauses must be included in all contracts where personal data is likely to be passed to a third party.

All paper based personal data must be held in lockable storage, whether on or off site.

Secure transfer of data and access out of school

The school/academy recognises that personal data may be accessed by users out of school/academy or transferred to the local authority or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school/academy or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school/academy
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location



- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of personal data

The school/academy should implement a document retention schedule that defines the length of time personal data is held before secure destruction. The Information and Records Management Society [Toolkit for schools](#) provides support for this process. The school/academy must ensure the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Demonstrating Compliance - Audit Logging / Reporting / Incident Handling

Organisations are required to keep records of processing activity. The data map referred to above will assist here. Records must include:

- the name and contact details of the data controller
- where applicable, the name and contact details of the joint controller and data protection officer
- the purpose of the processing
- to whom the data has been/will be disclosed
- description of data subject and personal data
- where relevant the countries it has been transferred to
- under which condition for processing the personal data has been collected
- under what lawful basis processing is being carried out
- where necessary, how it is retained and destroyed
- a general description of the technical and organisational security measures.

Clearly, in order to maintain these records good auditing processes must be followed, both at the start of the exercise and on-going throughout the lifetime of the requirement. Therefore, audit logs will need to be kept to:

- provide evidence of the processing activity and the DPIA
- record where, why, how and to whom personal data has been shared

- log the disposal and destruction of the personal data
- enable the school/academy to target training at the most at-risk data
- record any breaches that impact on the personal data

Fee

The school/academy should pay the relevant annual fee to the Information Commissioner's Office (ICO). Failure to renew may render the school/academy to a penalty in addition to other fines possible under the Data Protection Law.

Responsibilities

Every maintained school/academy is required to appoint a Data Protection Officer as a core function of 'the business'

The Data Protection Officer (DPO) can be internally or externally appointed.

They must have:

- expert knowledge
- timely and proper involvement in all issues relating to data protection
- the necessary resources to fulfil the role
- access to the necessary personal data processing operations
- a direct reporting route to the highest management level

The data controller must:

- not give the DPO instructions regarding the performance of tasks
- ensure that the DPO does not perform a duty or role that would lead to a conflict of interests
- not dismiss or penalise the DPO for performing the tasks required of them

As a minimum a Data Protection Officer must:

- inform, as necessary, the controller, a processor or an employee of their obligations under the data protection laws
- provide advice on a data protection impact assessment
- co-operate with the Information Commissioner
- act as the contact point for the Information Commissioner
- monitor compliance with policies of the controller in relation to the protection of personal data
- monitor compliance by the controller with Data Protection Law



The school/academy may also wish to appoint a Data Manager. Schools/academies are encouraged to separate this role from that of Data Protection Officer, where possible. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's / academy's information risk policy and risk assessment
- oversee the System Controllers

The school/academy may also wish to appoint System Controllers for the various types of data being held (e.g. learner information / staff information / assessment data etc.). System Controllers will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose
- how information has been amended or added to over time, and
- who has access to the data and why.

Everyone in the school/academy has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor (either in the school/academy or elsewhere if on school/academy business).

Training & awareness

All staff must receive data handling awareness / data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through:

- Induction training for new staff
- Staff meetings / briefings / INSET
- Day to day support and guidance from System Controllers

Freedom of Information Act

All schools / academies must have a Freedom of Information Policy which sets out how it will deal with FOI requests. FOI aims to increase transparency and accountability in public sector organisations as part of a healthy democratic process. Whilst FOI requests are submitted by an individual, the issue is for the school/academy to consider whether the requested information should be released into the public domain. FOI links to Data Protection Law whenever a request includes personal data. Good advice would encourage the school/academy to:

- delegate to the Headteacher day-to-day responsibility for FOI policy and the provision of advice, guidance, publicity and interpretation of the school's/academy's policy
- consider designating an individual with responsibility for FOI, to provide a single point of reference, coordinate FOI and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- consider arrangements for overseeing access to information and delegation to the appropriate governing body
- proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually
- ensure that a well-managed records management and information system exists in order to comply with requests
- ensure a record of refusals and reasons for refusals is kept, allowing the school/academy to review its access policy on an annual basis

Model Publication Scheme

The Information Commissioner's Office provides schools and organisations with a model publication scheme which they should complete. The school's / academy's publication scheme should be reviewed annually.

The ICO produce guidance on the model publication scheme for schools. This is designed to support schools / academies complete the Guide to Information for Schools.

Parental permission for use of cloud hosted services

Schools/academies that use cloud hosting services are advised to seek appropriate consent to set up an account for learners.

Use of Biometric Information

Biometric information is special category data. The Protection of Freedoms Act 2012, included measures that affect schools/academies that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools/academies under 18, they must obtain the written consent of a parent before they take and process their child's biometric data
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Law
- They must provide alternative means for accessing services where a parent or pupil has refused consent

New advice to schools/academies makes it clear that they are not able to use pupils' biometric data without parental consent. Schools/academies may wish to incorporate the parental

permission procedures into revised consent processes. (see Appendix Parent / Carer Acceptable Use Agreement)

Privacy and Electronic Communications

Schools/academies should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.

Electronic Devices - Searching & Deletion

Introduction

The changing face of information technologies and ever increasing pupil/student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.

Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The *Head Teacher/Principal* must publicise the school behaviour policy, in writing, to staff, parents/carers and students/pupils at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation - Advice for head teachers, staff and governing bodies" (2014 and updated January 2018)

<http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>

It is recommended that Headteachers/Principals (and, at the least, other senior leaders) should be familiar with this guidance.

Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

Responsibilities

The *Headteacher/Principal* is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher/Principal will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: insert relevant names/roles/group

The *Headteacher/Principal* has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data/files on those devices: (the policy should here list those staff/roles given such authority. A Headteacher/Principal may choose to authorise all staff willing to be authorised, but should consider training needs in making this decision).

The *Headteacher/Principal* may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Members of staff (other than Security Staff) cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.

Training/Awareness

It is essential that all staff should be made aware of and should implement the school's policy.

Members of staff should be made aware of the school's policy on "Electronic devices - searching and deletion":

- at induction
- at regular updating sessions on the school's online safety policy

Members of staff authorised by the Headteacher/Principal to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements

Search:

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data/files on those devices.

The school will already have a policy relating to whether or not mobile phones and other electronic devices are banned, or are allowed only within certain conditions. The school should therefore consider including one of the following statements in the policy:

Either:

Pupils/students are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school.

Or

Pupils/students are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school. (you should refer to the relevant policy or to list here the conditions under which they are allowed)

If pupils/students breach these roles:

Either:

The sanctions for breaking these rules will be: (list here)

Or

The sanctions for breaking these rules can be found in the (name the policy - for many schools this will be the Behaviour Policy)

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a *student/pupil* is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for. (Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training).

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties e.g. a visiting parent or contractor, only to devices in the possession of pupils/students.)

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the *student/pupil* being searched.

The authorised member of staff carrying out the search must be the same gender as the *student/pupil* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *student/pupil* being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a *student/pupil* of the opposite gender including without a witness present, but **only where you reasonably believe that there is a risk that serious harm will be caused to a person if you**

do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

The person conducting the search may not require the *student/pupil* to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the *student/pupil* has or appears to have control - this includes desks, lockers and bags. (schools will need to take account of their normal policies regarding religious garments/headwear and may wish to refer to it in this policy)

A student's/pupil's possessions can only be searched in the presence of the *student/pupil* and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force - force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

The examination of the data/files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff. The school may wish to add further detail about these arrangements.

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the SWGfL flow chart in the main School Template Policies document. Local authorities/local safeguarding partnerships may also have further guidance, specific to their area.

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. (It is recommended that members of staff should know who to contact, within school, for further guidance before taking action and that the person or persons is or are named within this policy).

A record should be kept of the reasons for the deletion of data/files. (DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the school can refer to relevant documentation created at the time of any search or data deletion in the event of a pupil /student, parental or other interested party complaint or legal challenge. Records will also help the school to review online safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices (particularly given the possible high value of some of these devices).

The school may wish to add a disclaimer to the relevant section of the Behaviour Policy which may assist in covering the school against damage/loss claims.

Audit/Monitoring/Reporting/Review

The responsible person (insert title) will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data/files. (a template log sheet can be found in the appendices to the School Online Safety Template Policies)

These records will be reviewed by ... (Online Safety Officer/Online Safety Committee/Online Safety Governor) at regular intervals (state the frequency).

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance and evidence gained from the records.

The school is required to publish its Behaviour Policy to parents annually (including on its website) - the Behaviour Policy should be cross referenced with this policy on search and deletion. DfE guidance can be found at:

<https://www.gov.uk/government/publications/searching-screening-and-confiscation>



Mobile Technologies Policy Template (inc. BYOD/BYOT)

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the pupils/students, staff and wider school/academy community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school/academy owned/provided or personally owned. The mobile technologies policy should sit alongside a range of policies including but not limited to the safeguarding policy, anti-bullying policy, acceptable use policy, policies around theft or malicious damage and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students/pupils that will prepare them for the high tech world in which they will live, learn and work.

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school/academy network, filtering of personal devices, breakages and insurance, access to devices for all students/pupils, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Schools/academies may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school/academy community - including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before

the school/academy embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

A range of mobile technology implementations is possible. The school/academy should consider the following statements and remove those that do not apply to their planned implementation approach.

- The school/academy acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- The school allows: (the school/academy should complete the table below to indicate which devices are allowed and define their access to school/academy systems)

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The academy recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school/academy, its staff, parents, carers and children.

Scope

This policy is subject to the academy's codes of conduct and acceptable use agreements.

This policy:

- **Applies to all staff and to all online communications which directly or indirectly, represent the academy.**
- **Applies to such online communications posted at any time and from anywhere.**
- Encourages the safe and responsible use of social media through training and education
- *Defines the monitoring of public social media activity pertaining to the academy*

The school/academy respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the academy name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the academy are outside the scope of this policy.

Digital communications with pupils/students are also considered. *Staff may use social media to communicate with learners via a academy social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control

Roles & Responsibilities

- **SLT**
 - Facilitating training and guidance on Social Media use.
 - Developing and implementing the Social Media policy
 - Taking a lead role in investigating any reported incidents.
 - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
 - Receive completed applications for Social Media accounts
 - Approve account creation
- **Administrator/Moderator**
 - Create the account following SLT approval
 - Store account details, including passwords securely
 - Be involved in monitoring and contributing to the account
 - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
 - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
 - Attending appropriate training
 - Regularly monitoring, updating and managing content he/she has posted via school/academy accounts
 - Adding an appropriate disclaimer to personal accounts when naming the school/academy

Process for creating new accounts

At his current point in time, the academy considers that the school website (www.scotholme.com), ClassDojo and the school's YouTube Channel (<https://www.youtube.com/channel/UCWong-zys9qE20kJiO6za5Q>) are the means to communicate. When considering any new channels of communication, the following will be taken into account:

- The aim of the account

- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the academy has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the academy, including volunteers or parents.

Monitoring

Academy accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school/academy social media account.

Behaviour

- **The academy requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy.** Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. Academy social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the academy.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media, staff must follow the academy media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school/academy and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school/academy policies. *The school/academy permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school/academy will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school/academy will deal with the matter internally. Where conduct is considered illegal, the school/academy will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school/academy, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school/academy users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school/academy protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

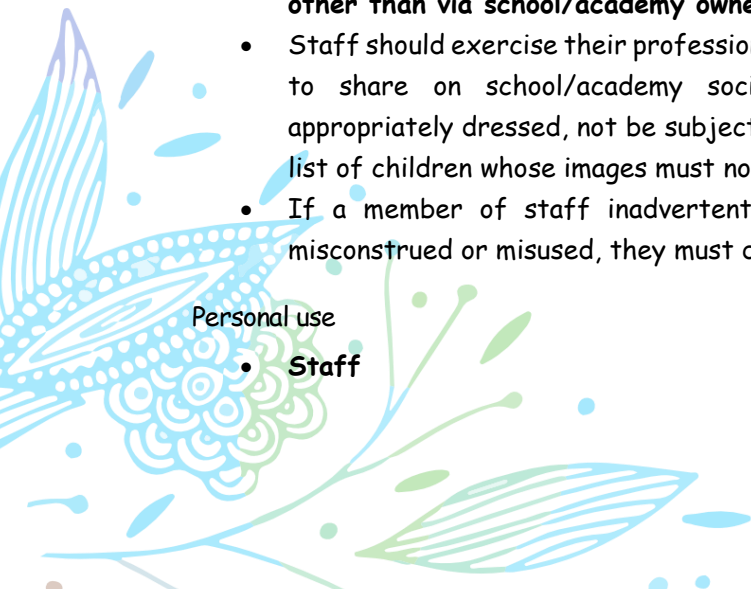
Use of images

School/academy use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought in line with the school's/academy's digital and video images policy.** If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload student/pupil pictures online other than via school/academy owned social media accounts**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school/academy social media accounts. Students/pupils should be appropriately dressed, not be subject to ridicule and must not be on any school/academy list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**



- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school/academy, it must be made clear that the member of staff is not communicating on behalf of the school/academy with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school/academy are outside the scope of this policy.
- Where excessive personal use of social media in school/academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *The school/academy permits reasonable and appropriate access to private social media sites.*
- **Pupil/Students**
 - **Staff are not permitted to follow or engage with current or prior pupils/students of the school/academy on any personal social media network account.**
 - The school's/academy's education programme should enable the pupils/students to be safe and responsible users of social media.
 - Pupils/students are encouraged to comment or post appropriately about the school/academy. Any offensive or inappropriate comments will be resolved by the use of the school's/academy's behaviour policy
- **Parents/Carers**
 - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
 - The school/academy has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
 - Parents/Carers are encouraged to comment or post appropriately about the school/academy. In the event of any offensive or inappropriate comments being made, the school/academy will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's/academy's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school/academy.
- The school/academy should effectively respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school/academy logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private

- Regularly review your connections - keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images - do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school/academy social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the school/academy into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school/academy accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Acknowledgements

With thanks to Rob Simmonds of Well Chuffed Comms (wellchuffedcomms.com) and Chelmsford College for allowing the use of their policies in the creation of this policy.



Online Safety Group Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from the [school/academy] community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the school/academy this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Full Governing Body.

2. Membership

2.1. The online safety group will seek to include representation from all stakeholders.

The composition of the group should include (N.B. in small schools/academies one member of staff may hold more than one of these posts):

[add/delete where appropriate]

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Online safety coordinator (not ICT coordinator by default)
- Governor
- Parent/Carer
- ICT Technical Support staff (where possible)
- Community users (where appropriate)
- *Student/pupil representation - for advice and feedback. Student/pupil voice is essential in the make-up of the online safety group, but students/pupils would only be expected to take part in committee meetings where deemed relevant.*

2.2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;

- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings

Meetings shall be held [insert frequency] for a period of [insert number] hour(s). A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the Online Safety Lead (or other relevant person) with the following [add/delete where relevant]:

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- To co-ordinate consultation with the whole school/academy community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through [add/delete as relevant]:
 - Staff meetings
 - Student/pupil forums (for advice and feedback)
 - Governors meetings
 - Surveys/questionnaires for students/pupils, parents/carers and staff
 - Parents evenings
 - Website/VLE/Newsletters
 - Online safety events
 - Internet Safety Day (annually held on the second Tuesday in February)
 - Other methods
- To ensure that monitoring is carried out of Internet sites used across the school/academy
- To monitor filtering/change control logs (e.g. requests for blocking/uN.B.locking sites).
- To monitor the safe use of data across the school/academy
- To monitor incidents involving cyberbullying for staff and pupils

6. Amendments

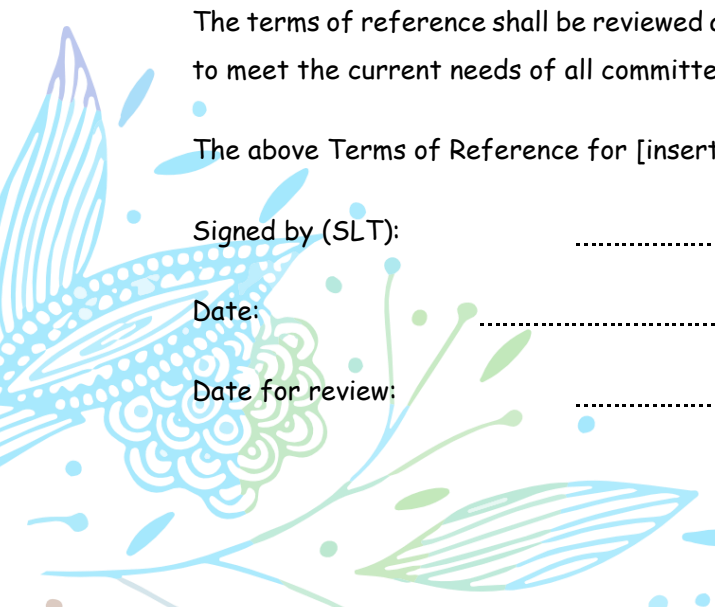
The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for [insert name of organisation] have been agreed

Signed by (SLT):

Date:

Date for review:



Legislation

Schools/academies should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

School/academies may wish to view the National Crime Agency website which includes information about "Cyber crime - preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

- Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:
 - Facilitate the secure transfer of information within the European Union.
 - Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
 - Give the public confidence about how businesses can use their personal information.

- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

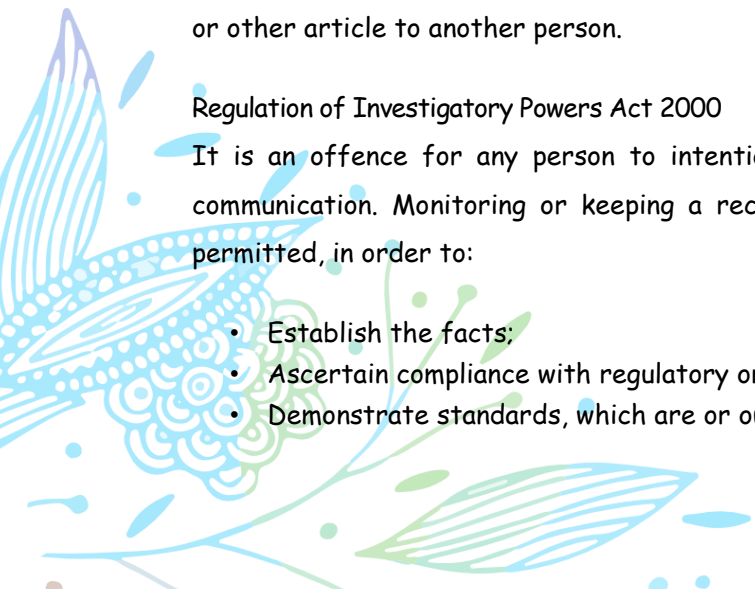
Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;



- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression

- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance -

<http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn - as it is now commonly known - involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the [Revenge Porn Helpline](#)

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre - <https://www.saferinternet.org.uk/>

South West Grid for Learning - <https://swgfl.org.uk/products-services/online-safety/>

Childnet - <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Revenge Porn Helpline - <https://revengepornhelpline.org.uk/>

Internet Watch Foundation - <https://www.iwf.org.uk/>

Report Harmful Content - <https://reportharmfulcontent.com/>

CEOP

CEOP - <http://ceop.police.uk/>

ThinkUKnow - <https://www.thinkuknow.co.uk/>

Others

[LGfL - Online Safety Resources](#)

[Kent - Online Safety Resources page](#)

INSAFE/Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Internet Safety (UKCIS) - <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

Netsmartz - <http://www.netsmartz.org/>

Tools for Schools

Online Safety BOOST - <https://boost.swgfl.org.uk/>

360 Degree Safe - Online Safety self-review tool - <https://360safe.org.uk/>

360Data - online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - <http://testfiltering.com/>

UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable - European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

SELMA - Hacking Hate - <https://selma.swgfl.co.uk>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour - <http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyber_bullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet - Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet - Project deSHAME - Online Sexual Harrassment](#)

[UKSIC - Sexting Resources](#)

Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>

[Ditch the Label - Online Bullying Charity](#)

[Diana Award - Anti-Bullying Campaign](#)

Social Networking

Digizen - [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

[Children's Commissioner, TES and Schillings - Young peoples' rights on social media](#)

Curriculum

SWGfL Evolve - <https://projectevolve.co.uk>

[UKCCIS - Education for a connected world framework](#)

Teach Today - www.teachtoday.eu/

Insafe - [Education Resources](#)

Data Protection

[360data - free questionnaire and data protection self review tool](#)

[ICO Guides for Education \(wide range of sector specific guides\)](#)

[DfE advice on Cloud software services and the Data Protection Act](#)

[IRMS - Records Management Toolkit for Schools](#)

[NHS - Caldicott Principles \(information that must be released\)](#)

[ICO Guidance on taking photos in schools](#)

[Dotkumo - Best practice guide to using photos](#)

Professional Standards/Staff Training

[DfE - Keeping Children Safe in Education](#)

[DfE - Safer Working Practice for Adults who Work with Children and Young People](#)

[Childnet - School Pack for Online Safety Awareness](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure/Technical Support

[UKSIC - Appropriate Filtering and Monitoring](#)

[SWGfL Safety & Security Resources](#)

Somerset - [Questions for Technical Support](#)

NCA - [Guide to the Computer Misuse Act](#)

NEN - [Advice and Guidance Notes](#)

Working with parents and carers

[Online Safety BOOST Presentations - parent's presentation](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops/education](#)

[Internet Matters](#)

Prevent

[Prevent Duty Guidance](#)

[Prevent for schools - teaching resources](#)

[NCA - Cyber Prevent](#)

Childnet - [Trust Me](#)

Research

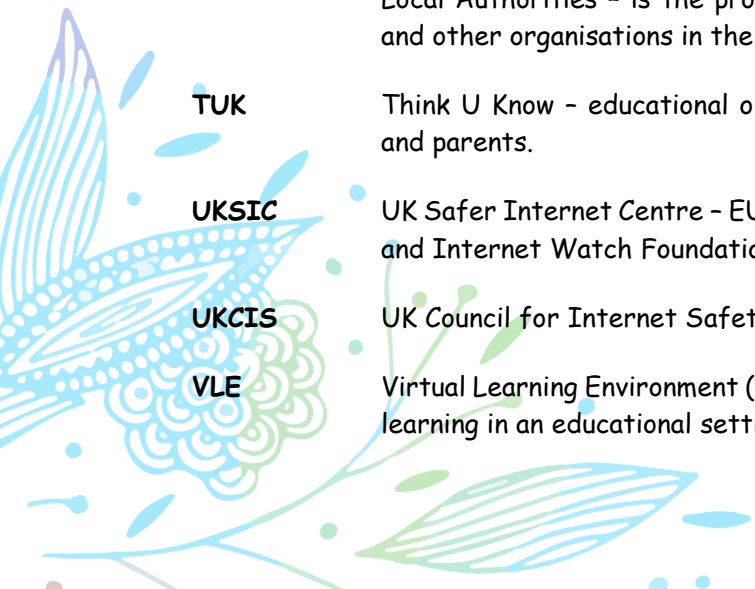
[Ofcom -Media Literacy Research](#)

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](#)



Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement - see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network - works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust - the Regional Broadband Consortium of SW Local Authorities - is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know - educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre - EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,



WAP Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS [Education for a Connected World Framework](#)

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Copyright of these Template Policies is held by SWGfL. Schools / Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy writing, review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in April 2018. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© South West Grid for Learning Trust Ltd 2018

