Online Safety Policy

February 2023

Contents

Introduction
School Online Safety Policy
Development, monitoring and review of the Policy
Schedule for development, monitoring and review
Scope of the Policy

Roles and Responsibilities
- Governors
- Headteacher and Senior Leaders
- Online Safety Coordinator / Officer
- Network Manager / Technical Staff
- Teaching and Support Staff
- Child Protection / Safeguarding Designated Person / Officer
- Online Safety Committee
- Pupils
- Parents / Carers
- Community Users

Online Safety - KCSIE the Four Cs

Policy Statements
- Education – Pupils
- Education – Parents / Carers
- Education – The Wider Community
- Education and training – Staff / Volunteers
- Training – Governors
- Technical – infrastructure / equipment, filtering and monitoring
- Use of digital and video images
- Data protection
- Communications
- Social Media - Protecting Professional Identity
- User Actions - unsuitable / inappropriate activities
- Responding to incidents of misuse

Related Policies:
- Safeguarding Policy
- Remote Learning Policy
- Social Media Policy
- Information Security Policy
- Electronic Information and Communications Policy
- Acceptable Use Policy and Agreement (Staff & Governors)
- Bring Your Own Device Policy
- Data Protection Policy
- Data Retention Policy

Appendices:
- Pupil Acceptable Use Policy Agreement Template – older children
- Pupil Acceptable Use Policy Agreement Template – younger children
- Parents / Carers Acceptable Use Policy Agreement Template
- Use of Digital Images and Videos
- Use of Cloud Permissions
- Staff and Volunteers Acceptable Use Agreement
- Community Users Acceptable Use Agreement
- FS/KS1 Online Safety Rules
- KS2 Online Safety Rules
- Safe Blogging Rules

- Responding to incidents of misuse – flowchart
- School Reporting Log template
- School Training Needs Audit template
- School Technical Security Policy (includes password security and filtering)
- School Policy Template – Electronic Devices – Search and Deletion
- School Online Safety Group Terms of Reference
- Legislation
- Links to other organisations and documents
- Glossary of Terms

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by consultation with

- Headteacher / Senior Leaders
- Online Safety Lead / Subject Leader / Middle Leaders
- Staff – including Teachers, Support Staff, Technical Staff
- Governors
- Parents and Carers

Consultation with the whole school community has taken place through a range of formal and informal meetings. This is an ongoing process due to the ever-changing nature of Online Safety.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the *Governing Body / Governors Sub Committee on:*	February 2022
The implementation of this Online Safety policy will be monitored by the:	*Safeguarding Governor, Senior Leadership Team and Middle Leaders*
Monitoring will take place at regular intervals:	*Monthly*
The *Governing Body / Governors Sub Committee* 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:	*Annually*
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:	*September 2023*
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer – ICT Support (if needed) Social Services, police etc*

The school will monitor the impact of the policy using:

- Logs of reported incidents (SLT)
- Monitoring logs of internet activity (including sites visited) (On-site Technical Support Person)
- Internal monitoring data for network activity (On-site Technical Support Person)
- Surveys / questionnaires of
    - pupils
    - parents / carers
    - staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* 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 school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix). In the case of both acts, action can only be taken over issues covered by the Behaviour Policy

The school will deal with such incidents within this policy in addition to the associated safeguarding (including our prevent strategy+), 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 school:

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 Teaching and Learning Sub Committee receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety. The role of the Online Safety Governor will include:

- meetings with members of the online safety committee school council
- regular meetings with the member(s) of SLT
- regular monitoring of Online Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meetings

Headteacher and Senior Leaders:

- **The Headteacher has a duty of care for ensuring the safety (including Online Safety) of members of the school community**; the day to day responsibility for Online Safety will be delegated to all Staff.
- **The Headteacher and at least one other 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 flowchart on dealing with Online Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR).
- The Headteacher / Senior Leaders are responsible for ensuring that Year Leaders 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 / Senior Leaders 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 those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from Year Leaders.

Online Safety Lead / Computing Team:

- leads the Online Safety Group
- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place this will include online networking and radicalisation. (see Prevent Strategy)
- provides training and advice for staff
- liaises with the Local Authority if necessary
- liaises with technical support staff
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments,
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering control logs.
- attends relevant training and committee of Governors meetings
- reports regularly to other members of the Senior Leadership Team

Network Manager / Technical staff:

The Network Manager / Technical Staff for Computing are responsible for ensuring (High Impact):

- **that the school's technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets required Online Safety technical requirements and any statutory guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are changed where and when appropriate**
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (currently the responsibility of High Impact and the broadband provider)
- 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 / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; Online Safety Lead for investigation / action / sanction. The approach needs to be evaluated regularly in light of new developments and methods.
- that monitoring software / systems are implemented and updated as agreed in school policies this will include online networking and radicalisation. (see Prevent Strategy)

Teaching and Support Staff

are responsible for ensuring that:

- **they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP/AUA)**
- **they report any suspected misuse or problem to the Headteacher / Senior Leader; Online Safety Lead 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**
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety and acceptable use policies
- 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. This includes the Prevent Strategy.
- In lessons where internet use is pre-planned, 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.

Designated Safeguarding Lead (Headteacher)

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
- radicalisation

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the *school* community, with responsibility for issues regarding Online Safety and the monitoring of the Online Safety policy including the impact of initiatives. The group is also responsible for reporting to the *Governing Body*.

Members of the Online Safety Group will assist the Online Safety Lead 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 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 *school* digital technology systems in accordance with the Pupil Acceptable Use Policy.
- 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 *school's* Online Safety Policy covers their actions out of school, if related to their membership of the school.
- will experience Online Safety training as part of their curriculum each year.

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 *school* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / Class Dojo and information about national / local Online Safety campaigns / literature.* Parents and carers will be encouraged to support the *school* 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 / Learning Platform and on-line / pupil records
- their children's personal devices in and beyond the school (where this is allowed)

Students/Work Experience/Volunteers/Community Users

Students/Work Experience/Volunteers/Community Users who access school systems / website / Learning Platform as part of the wider *school* provision will be expected to sign a Community User AUA (Acceptable Use Agreement) before being provided with access to school systems.

Online Safety

It is essential that children are safeguarded from potentially harmful and inappropriate online material. We recognise an effective whole school approach to online safety empowers us to protect and educate our pupils and staff in their use of technology whilst establishing mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk (KCSIE 22 para 136):

content:

being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, misandry, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact:

being subjected to harmful online interaction with other users; for example:
peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct:

online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

commerce:

risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Policy Statements

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 is therefore an essential part of the school'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 should be provided as part of Computing / PSHE / other lessons and should be regularly revisited
- Key Online Safety messages should be reinforced as part of a planned programme of lessons, assemblies and class council and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information. (Critical thinking)
- 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 taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil **Acceptable Use Agreement** and encouraged to adopt safe and responsible use both within and outside school.
- 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 and insist on the use of safe search engines.**
- **It is accepted that from time to time, for good educational reasons, pupils may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) 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 on-line 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 school will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, website, Learning Platforms, Class Dojo, Email, SMS*
- *Parents / Carers Drop-ins/sessions*
- *High profile events / campaigns e.g.* ***Safer Internet Day***
- *Reference to the relevant web sites / publications e.g.* **www.saferinternet.org.uk/** **http://www.childnet.com/parents-and-carers** (see school website and appendix for further links / resources)

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school'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 grandparents and other relatives as well as parents.
- The school website will provide Online Safety information for the wider community
- Where and when appropriate supporting community groups e.g. Early Years Settings, Child-minders, 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 regularly.**
- **All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreements.**
- *The Online Safety Lead will receive regular updates through attendance at external training events (e.g. from LA / other relevant organisations) 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 Lead will provide advice / guidance / training to individuals as required.*

Training – Governors / Directors

Governors / Directors 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 / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school 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 previous sections will be effective in carrying out their Online Safety 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 (Server Room).**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **All users will be provided with a username and secure password** by **in-house technical support** who will keep an up to date record of users and their usernames. Staff users are responsible for the security of their username and password and will be required to change their password where and when appropriate.

- **The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place.**
- The School Business Manager in liaison with the technician **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 is filtered by the broadband/filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored by High Impact
- There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- School SLT and 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 Agreement. (see appendix)
- Securus is used to monitor online activity across the school network - Securus provides specialist, online safety, designed to accurately monitor, respond and safeguard the welfare and wellbeing of digital users
- 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 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 for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- *An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.*
- *An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.* (see School's Information Security Policy and Data Protection Policy)

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 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.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and interrelated 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 school'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	Pupil owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only				*No*	*Yes*	*Yes*
No network access				*No*	*No*	*No*

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 Online Bullying 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.**
- 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 *pupils* in the digital / video images.
- *Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.* ***Those images should only be taken on school 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 school into disrepute.*
- *Pupils must not take, use, share, publish or distribute images of others without their permission.*
- *Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.*
- *Permission from parents or carers will be obtained before photographs of pupils are published on the school website (*covered as part of the AUA signed by parents or carers at the start of Foundation Stage or when the child joins the school - see Parents / Carers Acceptable Use Agreement in the appendix)
- *Pupil's work can only be published with the permission of the / pupil and parents or carers.*

Data Protection

In accordance with the requirements set out in the General Data Protection Regulations (GDPR), personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- **It will hold 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.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".** (see Privacy Notice on the school website)
- **It has a Data Protection Policy**
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

A child's personal data merits particular protection under the GDPR. Children have the same rights as adults over their personal data which they can exercise as long as they are competent to do so. Where a child is not considered to be competent, an adult with parental responsibility may usually exercise the child's data protection rights on their behalf. We comply with all the requirements of the GDPR, not just those specifically relating to children.

- We design our processing with children in mind from the outset, and use a data protection by design and by default
- approach.
- We make sure that our processing is fair and complies with the data protection principles.
- As a matter of good practice, we use DPIAs (Data Protection Impact Assessment) to help us assess and mitigate the risks
- to children.
- If our processing is likely to result in a high risk to the rights and freedom of children, then we always do a DPIA.
- When relying on consent, we make sure that the child understands what they are consenting to, and we do not exploit any imbalance of power in the relationship between us.
- When relying on 'necessary for the performance of a contract', we consider the child's competence to understand what
- they are agreeing to, and to enter into a contract.
- When relying upon 'legitimate interests', we take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place.
- We take into account sector specific guidance on marketing, such as that issued by the Advertising Standards Authority, to make sure that children's personal data is not used in a way that might lead to their exploitation.
- We comply with the direct marketing requirements of the Privacy and Electronic Communications Regulations (PECR).
- If we do use children's personal data to make such decisions, then we make sure that one of the exceptions in Article 22(2) applies and that suitable, child appropriate, measures are in place to safeguard the child's rights, freedoms and legitimate interests.
- We follow the approach in the ICO's Data Sharing Code of Practice.
- Our privacy notices are clear, and presented in plain, age-appropriate language.
- As a matter of good practice, we explain the risks inherent in the processing, and how we intend to safeguard against
- them, in a child friendly way, so that children (and their parents) understand the implications of sharing their personal data.
- We tell children what rights they have over their personal data in language they can understand.
- We design the processes by which a child can exercise their data protection rights with the child in mind, and make them easy for children to access and understand.
- We allow competent children to exercise their own data protection rights.
- If our original processing was based on consent provided when the individual was a child, then we comply with requests for erasure whenever we can.
- We design our processes so that, as far as possible, it is as easy for a child to get their personal data erased as it was for them to provide it in the first place.

Staff must ensure that they:

- At all times take great care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- Can help data subjects understand their rights and know how to handle a request whether verbal or written.
- Know who to pass it to in the school
- Will not transfer any school/academy personal data to personal devices except as in line with school policy
- 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 or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected, **therefore, their use is prohibited for this purpose)**
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school 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:

	School Staff				Pupils			
Communication Technologies	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 school	✓				✓ Special Circumstances -Left at Reception on arrival and collected on departure.			
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time i.e. lunch break		✓ Not to be used when with pupils						✓
Taking photos on mobile phones / cameras				✓				✓
Use of other mobile devices e.g. tablets, gaming devices		✓				✓		
Use of personal email addresses in school, or on school network				✓				
Use of school email for personal emails				✓				
Use of messaging apps		✓					✓ School System	
Use of social media		✓					✓ School System	
Use of blogs		✓					✓ School System	

Staff use personal devices for personal use.

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

- **The official *school* 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 school email service to communicate with others when in school, or on school systems (e.g. by remote access).*
- **Users must immediately report, to the nominated person – in accordance with the school 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 (Dojo, email, chat, Learning Platform etc.) must be professional in tone and content.** *These communications may only take place on official (monitored) school* 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 KS1, while pupils at KS2 may be provided with individual school email addresses for educational use.

- 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 school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/ and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Ensuring Personal information is not published
- Training to include: 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.

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school 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 *school* or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer (SLT) and Online Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

The School's *Social Media Agreement* should also be read in conjunction with this policy.

When official school social media accounts are established there should be:

- *A process for approval by senior leaders*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *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 school/academy disciplinary procedures*

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school 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 excessive personal use of social media in school 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*

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to proactively 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 *school'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.

Unsuitable / inappropriate activities

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	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 and 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: ● 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
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 school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. 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			

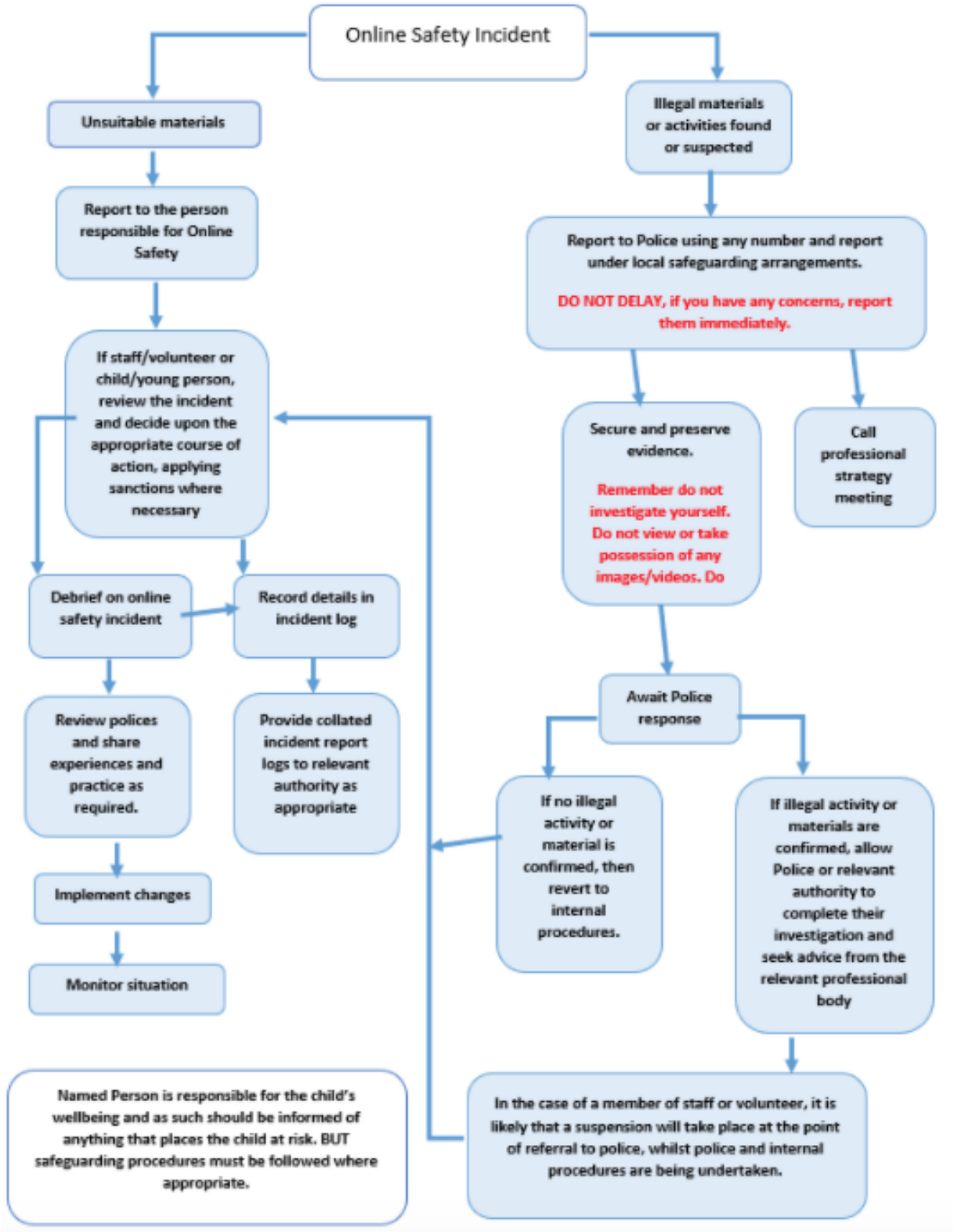
Use of video broadcasting e.g. YouTube			**X**			

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" on previous page).

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 school community will be responsible users of digital technologies, who understand and follow school 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 / volunteer 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 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
    - offences under the Computer Misuse Act (see chart)
    - 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 *school* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school 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:

Pupils	Possible Actions / Sanctions								
Incidents:	Refer to class teacher	Refer to Year Leader/ Deputy Head	Refer to Headteacher / SLT	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			
Unauthorised use of non-educational sites during lessons	X	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X							X	
Unauthorised use of social media / messaging apps / personal email		X	X					X	X
Unauthorised downloading or uploading of files		X	X					X	X
Allowing others to access school network by sharing username and passwords	X	X	X			X		X	
Attempting to access or accessing the school network, using another 's / pupil's account			X			X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff		X	X			X	X	X	X
Corrupting or destroying the data of other users		X	X			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
Continued infringements of the above, following previous warnings or sanctions		X	X			X			X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X	X		X	X		X
Using proxy sites or other means to subvert the school's filtering system			X		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	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X	X	X	X	X	X	X

Staff	Possible Actions / Sanctions							
Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Tec support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
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	X	X **If necessary**		X	X		
Unauthorised downloading or uploading of files	X	X			X	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	X			X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X			X	X		
Deliberate actions to breach data protection or network security rules		X	X	X	X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	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
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with s / pupils		X	X	X				X
Actions which could compromise the staff member's professional standing		X	X		X			X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X	X		X			X
Using proxy sites or other means to subvert the school's / academy's filtering system		X	X		X			X
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X	X		
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X			X
Breaching copyright or licensing regulations		X			X	X		
Continued infringements of the above, following previous warnings or sanctions		X	X					X

Appendices

Appendices

Can be found on the following pages:

- Pupil Acceptable Use Agreement template (older children) 23
- Pupil Acceptable Use Agreement template (younger children) 25
- Parents / Carers Acceptable Use Agreement template 26
- Parents/Carers Use of digital images and Videos 27
- Use of Cloud permissions 28
- Staff and Volunteers Acceptable Use Agreement 29
- Community Users Acceptable Use Agreement 31
- EYFS and KS1 Online Safety Rules 32
- KS2 Online Safety Rules 33
- Safe Blogging Rules 34
- Record of reviewing sites (for internet misuse) 35
- School Reporting Log template 36
- School Training Needs Audit template 36
- School Technical Security Policy template including Filtering 37
- Electronic Devices, Search and Deletion 42
- Legislation 46
- Links to other organisations and documents 49
- Glossary of terms 51

Pupil Acceptable Use Agreement for Key Stage 2 Pupils

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 internet access at all times.

This Acceptable Use Policy 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 users at risk.

The school will try to ensure that *pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my own personal safety:

- I understand that the *school* 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* systems and devices are primarily intended for educational use and that I will not use them for personal 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* systems or devices for on-line gaming, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

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*:

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the *school*, 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.
- 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. Google Classroom and relevant Blogging Tool

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* 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 cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, internal exclusion, fixed term exclusion, 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.

Signed (child):……

Signed (parent): ……..

Pupil Acceptable Use Policy Agreement – 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
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer 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/iPad.

Signed (child):……

Signed (parent): ……..

Parent / Carer
Acceptable Use Agreement

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

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications 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 users at risk.
- that parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users. A copy of the / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work. (Schools will need to decide whether or not they wish parents to sign the Acceptable Use Agreement on behalf of their child)

Permission Form

Parent / Carers Name _____ Pupil Name _____

As the parent / carer of the above *pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

Either: (KS2 and above)
I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
Or: (KS1)
I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, Online Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's Online Safety.

Signed _____ _____

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. 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,

The school will comply with the Data Protection Act and request parents / 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 in 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.

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

Digital / Video Images Permission Form

Parent / Carers Name	
Pupil Name	

As the parent / carer of the above *pupil*, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.	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	

Use of Cloud Systems Permission Form

The school uses Google Classroom / Apps for Education and other online learning tools for *pupils* and staff. This permission form describes the tools and pupil / responsibilities for using these services.

The following services are available to each *pupil* and hosted by Google as part of the school's online presence in Google Apps for Education:

Mail - an individual email account for school use managed by the school

Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments

Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office

Sites - an individual and collaborative website creation tool

Using these tools, *pupils* collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of pupil use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

The school believes that use of the tools significantly adds to your child's educational experience.

As part of the conditions we are required to seek your permission for your child to have a Google Apps for Education account:

Parent / Carers Name

Pupil Name

As the parent / carer of the above *pupil*, I agree with my child using the school using Google Apps for Education. Yes / No

Signed

Date

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New and constantly changing technologies have become integral to the lives of children and young people in today's society, both within schools 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 internet access 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 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 technology to enhance their work, to enhance learning opportunities for *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 school systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that 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 *school* will monitor my use of the school systems, email and other digital communications tools..
- I understand that the rules set out in this agreement also apply to use of school digital systems (eg laptops, email, Learning Platform etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital 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.
- 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* 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 / Learning Platform) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. 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*:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* 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 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 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 policies.
- I will not disable or cause any damage to school 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 School/ LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or 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 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*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school technology equipment in school, but also applies to my use of school 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.
- I understand that if I fail to comply with this Acceptable Use Policy 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 digital technologies will be responsible users and stay safe while using these systems and devices
- that school 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 risk 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.

- I understand that my use of school systems and devices and digital communications 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 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 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 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 has the right to remove my access to school systems / devices

I have read and understand the above and agree to use the school ICT 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

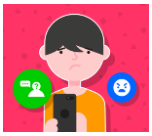
Signed

Date

Liscard Primary School's
EYFS and KS1 Online Safety Code
Think before you click…

	We only use the programs or Apps our teacher asks us to use.
	We only go online when an adult asks us.
	We only click on the buttons or links when we know what they do.
	We can search online when with an adult.
	We always ask if we get lost on the Internet.
	We can only send messages and emails together with an adult.

Liscard Primary School's
KS2 Online Safety Code
Think before you click…

	We ask permission before using the internet.
	We only use websites our teacher has chosen.
	We tell an adult if we see anything we are uncomfortable with.
	We immediately close any webpage we are uncomfortable with.
	We send emails/messages that are polite and friendly. We only email/message people an adult has approved. We do not open emails sent by anyone we don't know.
	We never share personal information or passwords.
	We never arrange to meet anyone we don't know.
	We only use school based chat platforms or messaging.

Safe Blogging Rule	
We have a few simple guidelines that we need to keep to in order to make the most of our school blog.	
1	Children are to only use their first name when commenting. *(You could also do this on other websites. Maybe use a nickname, not your real name. e.g. FootyBoy123)*
2	Parents who leave comments are asked to use their first name only so as not to identify their child. Or post comments as “Jack’s Mum” or “Juliet's Grandfather”.
3	All posts will be checked by a teacher before they are published to the blog.
4	All comments are moderated by a teacher before they appear on the blog.
5	Always be respectful of other people's work - be positive if you are going to comment.
6	All posts should relate to school life and should not include any personal details or information about individual pupils, staff, parents or carers.
7	No text talk please - write in full sentences and read your comments back carefully before submitting.

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	

Reporting Log

Group:

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

Training Needs Audit Log

Group:

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

School Technical 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 an impact on policy and practice.

As the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the Online Safety measures that might otherwise be carried out by the *school* itself (as suggested below). It is also important that the managed service provider is fully aware of the *school* Online Safety Policy / Acceptable Use Agreements). The *school* will also check the Local Authority / other relevant body policies / guidance on these technical issues.

Responsibilities

The management of technical security will be the responsibility of the IT Technician (High Impact) and Julie Forsyth (School Business Manager)

Technical Security

Policy statements

The school will be responsible for ensuring that the school 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 will 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 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 technical systems.** *Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed, at least annually, by the Online Safety Committee (or other group).*
- 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. *(See Password section below).*
- *The IT Technician and Julie Forsyth* 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- *Mobile device security and management procedures are in place.*
- *School 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 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 Lead / 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 system.
- *An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users.*
- *An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school 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 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 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 technical systems, including networks, devices, email and Learning Platforms.

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Online Safety Committee (or other group).
- **All school networks and systems will be protected by secure passwords that are regularly changed.**
- **The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the *Headteacher / Principal* or other nominated senior leader and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentication for such accounts**. (We should never allow one user to have sole administrator access)
- Passwords for new users, and replacement passwords for existing users will be allocated by the IT Technician (IT Support); any changes carried out must be notified to the manager of the password security policy (above).
- All users (adults and young people) will 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.
- Users will change their passwords at regular intervals – as described in the staff and pupil sections below.
- The level of security required may vary for staff and pupil accounts and the sensitive nature of any data accessed through that account.
- Requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user (the school will need to decide how this can be managed – possibly by requests being authorised by a line manager for a request by a member of staff or by a member of staff for a request by a pupil).

Staff passwords:

- **All staff users will be provided with a username and password** by *the IT Technician / School Business Manager who will keep an up to date record of users and their usernames.*
- *the password should be a minimum of 12 characters long and must include three of – uppercase character, lowercase character, number, special characters*
- *must not include proper names or any other personal information about the user that might be known by others*
- *the account should be "locked out" following six successive incorrect log-on attempts*
- *temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on*
- *passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)*
- *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*
- should be changed at least every 60 to 90 days.

- should not re-use for 6 months and be significantly different from the previous password. The *last four passwords cannot be re-used* passwords created by the same user.
- should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- should be different for systems used inside and outside of school

Pupil passwords

- **All users** (at KS1/2 and above) **will be provided with a username and password** by *(In house technical support) who will keep an up to date record of users and their usernames.*
- Users will be required to change their password regularly.
- Pupils will be taught the importance of password security.
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

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

- at induction.
- through the school's Online Safety policy and password security policy.
- through the Acceptable Use Agreement.

Pupils will be made aware of the school's password policy:

- in lessons.
- through the Acceptable Use Agreement.

Audit / Monitoring / Reporting / Review

The responsible person (In-house Technical Support and the School Business Manager) will ensure that full records are kept of:

- User Ids and requests for password changes.
- User log-on.
- 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 the members of the SLT. 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 and authorised by a second responsible person prior to changes being made (SLT).
- be reported to the Online Safety Group regularly in the form of an audit of the change control logs.

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 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.

- *The school maintains and supports the managed filtering service provided by the LA through their designated Internet Service Provider.*
- *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 (or other nominated senior leader).*
- *Mobile devices that access the school internet connection (whether school 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 LA.*
- *Requests from staff for sites to be removed from the filtered list will be considered by the technical* (and a member of the SLT). *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 will be made aware of the importance of filtering systems through the Online Safety education programme. 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:

- *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.

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 in-house technical support and SLT 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.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- *the SLT*
- *Online Safety Committee*
- *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.

Further Guidance

Schools may wish to seek further guidance. The following is recommended:
NEN Technical guidance: http://www.nen.gov.uk/advice/266/nen-guidance-notes.html

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"

School Policy: Electronic Devices - Searching & Deletion

Introduction

The changing face of information technologies and ever increasing pupil / 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* must publicise the school behaviour policy, in writing, to staff, parents / carers and 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"
http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

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* 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 will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: Senior Leadership team in collaboration with Key Governors

The *Headteacher* 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: All members of the SLT

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

Training / Awareness

Members of staff are 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 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.

Pupils 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. The sanctions for breaking these rules can be found in the Possible Actions/Sanctions part of this 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 *pupil* is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.

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

The authorised member of staff carrying out the search must be the same gender as the *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 *pupil* being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a *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 */ 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 *pupil* has or appears to have control – this includes desks, lockers and bags.

A pupil's possessions can only be searched in the presence of the *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 and 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.

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.

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, parental or other interested party complaint or legal challenge.

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).

Audit / Monitoring / Reporting / Review

The responsible person (Headteacher) 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.

These records will be reviewed by the *Online Safety Governor* at regular intervals.

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

Legislation

Schools 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 e 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.

Data Protection Act 2018

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 DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018.
It sits alongside the GDPR, and tailors how the GDPR applies in the UK - for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.
The GDPR is the General Data Protection Regulation (EU) 2016/679. It sets out the key principles, rights and obligations for most processing of personal data – but it does not apply to processing for law enforcement purposes, or to areas outside EU law such as national security or defence.
The GDPR came into effect on 25 May 2018. As a European Regulation, it 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.

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 helpline 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 TradeMarks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trademarks 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

The new 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 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:
http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations

Keeping Children Safe in Education. This is outlined on pages 32 to 35 and 150 to 152

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.

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:

Teaching online safety in school 2019
Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects

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 - 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/Cyberbullying_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

Teaching Online Safety in Schools

Online safety in schools and colleges: questions from the governing board

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 Commissioner's 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 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

Policy Evaluation

Points to be considered	Yes	No	N/A	Please supply evidence
• Policy annually reviewed	✓			Shared with all stakeholders, approved by governors and published on the school website
• Policy in line with current legislation	✓			Annual review to ensure any statutory changes or updates in policies are included.
• Coordinator in place	✓			Yes – SLT
• Nominated governor in place	✓			
• Coordinator carries out role effectively	✓			As identified through performance management and feedback from the headteacher
• Headteacher, coordinator and nominated governor work closely	✓			Regular meetings and updates to governors via sub committee
• Policy endorsed by governing body	✓			
• Policy regularly discussed at meetings of the governing body	✓			See governor meeting minutes
• School personnel aware of this policy	✓			
• School personnel comply with this policy	✓			
• Pupils aware of this policy	✓			Online Safety Agreements and Rules in Place and shared with Pupils
• Parents aware of this policy	✓			Published on the website
• Visitors aware of this policy	✓			SLT share relevant aspects with visitors
• Local community aware of this policy	✓			Published on the website
• Funding in place	✓			
• Policy complies with the Equality Act	✓			
• Equality Impact Assessment undertaken	✓			
• Policy referred to in the School Handbook		✓		
• Policy available from the school office		✓		On website but a paper copy can be printed on request
• Policy available from the school website	✓			
• School Council involved with policy development		✓		
• All stakeholders take part in questionnaires and surveys		✓		
• All associated training in place	✓			
• All outlined procedures complied with	✓			

• Linked policies in place and up to date	✓			
• Associated policies in place and up to date	✓			

A statement outlining the overall effectiveness of this policy
The policy ensures that all the school community are aware of the statutory duties around Online Safety and what is expected of all staff, pupils and parents to ensure that these duties are met. The policy clearly sets out how the school will support children through clear Online Safety procedures and curriculum planning.

Policy Approval Form

Policy Title:	Online Safety Policy						Date when written:		June 2022		
Policy written by:	Lindsey Moran				New Policy (√or x)			Revised Policy (√or x)	✓		
Stakeholders consulted in policy production: (√or x)	Governors	Senior Leadership Team	Teaching Personnel	Support Personnel	Administrative Personnel	Parents	Pupils	Local Community			
	✓	✓	✓	✓	✓						
Date when approved by Governors:	June 22		Date when presented to stakeholders:	June 22		Date when implemented:	June 22				
Published on: (√or x)	School Website			School Prospectus			Staff Handbook				
	✓										