Huntington CP School

Learn to Live
Live to Learn

E-Safety
(including Online Safety)
Policy
2023

CONTENTS

RATIONALE

New 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 and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

Risks

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Online bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this E-safety Policy is used in conjunction with other school policies (e.g. Behaviour, Anti-bullying and Safeguarding policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Safeguards

The school must demonstrate that it has provided the necessary safeguards to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks. The E-safety Policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

The requirement to ensure that children are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Huntington CP School will, through this policy, ensure that it meets its statutory obligations to ensure that children are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies.

In England, schools are subject to an increased level of scrutiny by Ofsted Inspectors during school inspections. From 2015, additional duties under the Counter Terrorism and Securities Act 2015 require schools to ensure that children are safe from terrorist and extremist material on the internet. Revised "Keeping Children Safe in Education" guidance obliges schools and colleges in England 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."

The school will review the E-Safety Policy every three years and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.
The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and Governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

ACKNOWLEDGEMENT

This policy is based on a template provided by SWGfL (first published October 2013, revised January 2020), which would like to acknowledge the contribution of a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of its online safety policy templates.

DEVELOPMENT & REVIEW OF THE POLICY

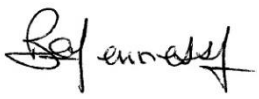
This E-safety Policy has been developed by the Premises and Health & Safety Committee, informed by discussions with teachers, support staff, parents and pupils.

Consultation with the whole school community has taken place through a range of formal and informal meetings, including staff meetings, school council meetings and parent consultation.

Policy Review

Committee responsible for Review: Premises & Health and Safety

Regularity of Review: every three years (or as required)

Signed:  Chair of Governors

Signed:  Headteacher

Date of Committee approval: 22/11/23

Next review date: Autumn 2026

SCOPE OF THE POLICY

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

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. This is relevant to incidents of online bullying, or other e-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 below, *Electronic Devices: Search and Deletion Policy*). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

ROLES AND RESPONSIBILITIES

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Governors
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Premises and Health & Safety Committee receiving regular information about e-safety incidents and monitoring reports. The role of Safeguarding Governor will include responsibility for e-Safety, and the latter will entail:

- termly meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- reporting to relevant Governors' committees

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety may be delegated to the E-Safety Co-ordinator (if different).
- The Headteacher and (at least) another member of the Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see below, *Responding to incidents of misuse*, and relevant Local Authority disciplinary procedures).
- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role (if the Headteacher does not perform this role, which currently they do). This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-Safety Coordinator

The E-Safety Coordinator (at present, the Headteacher):

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with the E-Safety Governor to discuss current issues and review incident logs
- attends relevant Governors' sub-committee meetings
- reports regularly to Senior Leadership Team

IT Support Staff

It is the responsibility of the school to ensure that the e-safety measures outlined below are carried out by the school's contracted IT support provider. It is also important that the IT support provider is fully aware of the school 's e-safety policy and procedures. The IT support staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority E-Safety Policy / Guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the school network/website/digital education platform/email system is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher/E-Safety Governor for investigation.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff and Volunteers Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher for investigation.
- all digital communications with pupils and parents should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities, in addition to being directly addressed within the Computing curriculum
- pupils understand and follow the e-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
- 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

The Designated Safeguarding Lead should be trained in e-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

At Huntington CP School, the Designated Safeguarding Lead is also the E-Safety Coordinator.

Pupils

Pupils:

- are responsible for using the school digital technology systems in accordance with the e-Safety rules
- 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
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- should not bring mobile devices, including mobile phones and digital cameras, into school, or take them on educational visits (the exception being Y5/6 pupils who walk to/from home alone, having received permission to do this, who may bring mobile phones into school for safekeeping by the class teacher throughout the school day – their use within school is not permitted)

Parents

Parents 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 parent workshops, newsletters and advice on the school website, including information about e-safety campaigns, both national and local. Parents will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events (see below, *Use of Digital & Video Images*)
- access to parents' sections of the school website and digital education platform

Parent volunteers

It will be made clear to parents accompanying pupils on visits that they are not to take photographs on portable devices, the expectation being that teachers will take photographs of such visits and make suitable images available to parents online, via the school website and Twitter account.

Community Users

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems (see Appendices).

POLICY STATEMENTS

EDUCATION AND TRAINING

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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

Teaching staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities, and will be provided in the following ways:

- A planned e-safety curriculum will be provided as part of the Computing curriculum: the school currently (2020) uses the scheme *Digital Literacy and Citizenship in a Connected Culture* (SWGfL, based on materials from Common Sense Media).
- Key e-safety messages should be reinforced regularly via assemblies and PSHE activities
- Children should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Children, especially in upper KS2, should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Children 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.
- Children should be helped to understand the need for the E-Safety 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 children 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 children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites visited.

Parents

Parents 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:

- Newsletters & school web site (including provision of relevant web links)
- Parent information evenings
- National / local events e.g. Safer Internet Day
- Involvement in curriculum activities

Staff & Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- **A programme of formal e-safety training** will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. The school has an annual subscription to SWGfL's BOOST service to provide access to professional development resources
- All new staff will receive e-safety training as part of their **induction programme**, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Coordinator will provide advice and training to individuals as required.

Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of the Premises and Health & Safety Committee. This may be offered in a number of ways:

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

TECHNICAL – INFRASTRUCTURE, ACCESS, PASSWORDS & FILTERING

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
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities
The management of technical security will be the responsibility of the Headteacher, and enacted via liaison with the IT technician.

Technical Requirements & Security

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- There will be regular reviews and audits of the safety and security of school technical systems
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, computers, laptops, *Chromebooks* and *Learnpad* tablets from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual computers are protected by up to date virus software (*Panda Security*).
- Technical incidents should be reported to the IT Support Staff via an entry in the IT file (yellow file kept in school office).
- Security breaches should be reported immediately to the E-Safety Co-ordinator.
- The Headteacher 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.

Access and Passwords

- All users will have clearly defined access rights to school technical systems and devices.
- All staff and KS2 pupil users will be provided with a username and secure password by the Headteacher, who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. KS1 and EYFS pupil users will generally use class log-ins and passwords.
- Staff passwords should be a minimum of 8 characters long and must include three of: uppercase character, lowercase character, number, special characters. Staff 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
- The administrator log-in details for the school IT system must also be available to the Headteacher and Deputy Headteacher, and kept for reference in the school safe**.**
- An agreed policy is in place for the provision of temporary access of guest users (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

Internet Filtering

- Internet access is filtered for all users by the Local Authority ISP.
- The filtering ensures that children are safe from terrorist and extremist material.
- There is a clear process in place to deal with requests for filtering changes.

Staff use

- An agreed policy is in place regarding the extent of personal use that staff are allowed on school devices that may be used out of school.
- Staff are not able to download executable files and install programs on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks).
- Staff may only use personal CDs/DVDs on school devices for curriculum purposes if the content is age appropriate (U certificate, in the case of BBFC classified video material)
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Pupil/family use

- An agreed policy is in place regarding the extent of personal use that pupils and family members are allowed on school devices that may be used out of school (e.g. *Chromebooks* supplied for remote learning)

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 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, as follows:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- **Written permission from parents or carers will be obtained before digital / video images of pupils are published on the school website (or elsewhere).**
- In accordance with guidance from the Information Commissioner's Office, parents 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 GDPR/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 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 exercised, 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, and the permission of teaching staff.
- 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 the school website, particularly in association with digital / video images.

DATA PROTECTION

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

The school will ensure that:

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

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

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

Staff must ensure that they:

- take care, at all times, to ensure the safe keeping 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 understands their rights and know how to handle a request whether verbal or written (knowing who to pass it to in the school)
- encrypt and password protect any mobile or other devices (including USBs) on which personal data is stored or transferred.
- will not transfer any school personal data to personal devices except as in line with school policy
- access personal data sources and records 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

COMMUNICATIONS

A wide range of rapidly developing communications technologies has the potential to enhance learning. 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 by the LA
- Users should be aware that email communications are monitored. Staff should use only the school email service to communicate with others when in school, or on school systems.
- Users must immediately report, to the Headteacher, 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 must be professional in tone and content. Such communications may only take place via the school email system: personal email addresses, text messaging or social media must not be used for these communications.
- Whole class email addresses will be used for pupils - individual pupils have been assigned school email addresses as a requirement of the implementation of *Google Classroom*, but these should not be used for communication purposes.
- Pupils should be taught about e-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

(see also the school's Social Media Policy)

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, engage in online bullying, 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:

- Ensuring that personal information is not published.
- Training to include: acceptable use; social media risks; checking of settings; data protection (under the GDPR); 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 their personal social media to pupils, parents 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.

Monitoring of Public Social Media

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

The school's use of social media for professional purposes will be checked regularly by the Headteacher to ensure compliance with other school policies (e.g. see section Use of Digital and Video images).

USER ACTIONS: UNSUITABLE / INAPPROPRIATE ACTIVITIES

The school believes that the activities referred to in the following section would be generally 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, other than as indicated. The school policy restricts usage as follows:

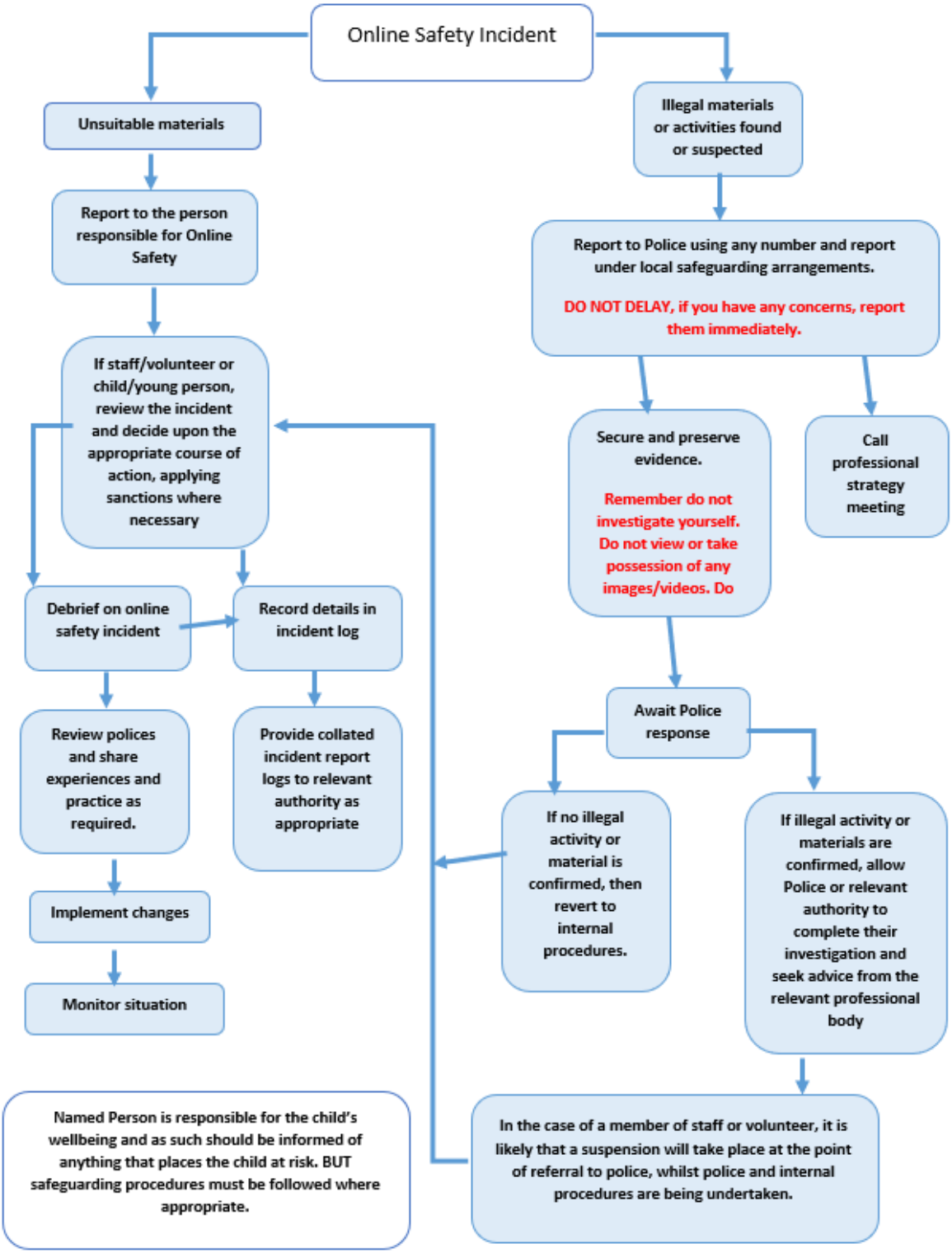
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on any material, remarks, proposals or comments that contain or relate to:	child 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 the UK: to stir up religious hatred, or hatred on the grounds of sexual orientation (contrary to the Public Order Act 1986)					X
	promotion of extremism or terrorism					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				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 systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Unfair usage (downloading / uploading large files that hinder others in their use of the internet)					X	
Using school systems to run a private business					X	
Infringing copyright					X	
On-line gaming (educational) – single player only (NOT multi-user)			X			
On-line gaming (non-educational) – single player only (NOT multi-user)			X			
On-line gambling					X	
On-line shopping / commerce (this is acceptable by school credit card holders for school purchases)				X		
File sharing			X			
Use of social media (other than school Twitter account)					X	
Use of messaging apps					X	
Use of video broadcasting e.g. YouTube (curriculum-related only)			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' table above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) 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, irresponsible or, very rarely, deliberate misuse.

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

- Have more than one senior member of staff involved in this process: this is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority 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 'User Actions' table above)
    - 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 safeguarding 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.

APPENDICES

E-Safety Agreement
E-Safety Rules: KS1, KS2
Staff (and Volunteer) Acceptable Use Policy Agreement
Community Users Acceptable Use Policy Agreement
Record of reviewing devices / internet sites
School Reporting Log
School Training Needs Audit
Electronic Devices: Searching and Deletion Policy
Legislation
Links to other organisations and documents
Glossary of Terms

Huntington CP School

E-Safety Agreement

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both **pupils and their parents/carers** are **asked to sign** to show that the E-Safety Rules, which have been revised in consultation with classes Y1-Y6, have been understood and agreed.

Pupil Name:	***Class:***

Pupil's Agreement

- I have read and I understand the school E-Safety Rules.
- I will use school computers, our school website, internet access and other new technologies in a responsible way at all times.
- I know that school computers, the school website and *Google Classroom* may be monitored.

Signed:	***Date:***

Parent's Consent for Web Publication of Work

I agree that my child's work may be electronically published (this does not refer to photographs including my child, for which separate permission must be sought).

Parent's Consent for Internet Access

I have read and understood the school E-Safety rules and give permission for my child to access the Internet and Google Classroom. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, including use of a filtered internet service provided by the Local Authority, but I appreciate that this is a difficult task. I understand that the school cannot be held responsible for the content of materials accessed through the Internet.

Signed:	***Date:***
Please print name:	

Please complete, sign and return to the school office.

Thank you

Think before you Click

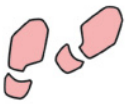
E-Safety Rules for Key Stage 1

These rules help us to stay safe on the Internet

We only use the Internet when an adult is with us, and we always ask if we get lost.

If we see something we don't like on the Internet we tell an adult straight away.

We only click on the buttons or links when we have been told what they do.



We never let anyone know our passwords (except for our parents).

We only write polite and friendly messages on the website and Google Classroom, to people that we know.

We Log Out when we finish work.

Think before you Click

E-Safety Rules for Key Stage 2

- We ask permission before using the internet.
- We immediately minimize any webpage we are uncomfortable with, and then tell an adult straight away.
- We only write polite and friendly messages on the website and Google Classroom, to people that we know.
- We tell an adult if someone sends us an unpleasant message.
- We never give out personal information or passwords, and we Log Out when we have finished working.
- We never upload photos of ourselves or other children.
- We never arrange to meet anyone we don't know.
- We never try to visit internet chat rooms.

STAFF (AND VOLUNTEER) ACCEPTABLE USE POLICY AGREEMENT

School Policy
New 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 technology systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for 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 technology systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the technology 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 e-safety and 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 digital technology and communication systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, tablets, email, school website and school Twitter account) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school (see table on p.17, *User Actions: unsuitable / inappropriate activities*)
- 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 that I become aware of to the appropriate person.

I will be professional in my communications and actions when using school digital technology 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 only use personal CDs/DVDs on school devices for curriculum purposes if the content is age appropriate (U certificate, in the case of BBFC classified video material)
- 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) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school.

- I will only communicate with pupils and parents 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 (e.g. mobile phone, USB device) 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 digital technology systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted (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 programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings.
- 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's policies. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper-based documents containing personal data must be held in lockable storage.
- I understand that data protection policy (under the GDPR) 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, either by making an entry in the IT file or informing the Headteacher directly.

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 school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school digital technology 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.

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** _____

Learn to Live
Live to Learn

COMMUNITY USERS ACCEPTABLE USE POLICY AGREEMENT

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 will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs 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 Headteacher.
- 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 programs of any type on a school device, nor will I try to alter computer settings.
- 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, to the Headteacher.
- 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 digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name	
Signed	
Date	

RECORD OF REVIEWING DEVICES / INTERNET SITES

(for Responding to Incidents of Misuse)

Class	
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

School Reporting Log

Reporting Log

Class .....

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

SCHOOL TRAINING NEEDS AUDIT

Training Needs Audit Log

Class: .....

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

ELECTRONIC DEVICES: SEARCHING & DELETION POLICY

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 Headteacher will; publicise the school behaviour policy, in writing, to staff, parents and pupils at least once a year. (There should therefore be clear links between the search policy and the behaviour policy).

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

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:
Deputy Headteacher
KS2 Lead

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

- at induction
- at regular updating sessions on the school's E-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 not allowed to bring mobile phones or other personal electronic devices to school, or take them on educational visits.

The only exception to this rule is for Y5/6 pupils who walk to/from home alone, and for whom parental permission for this has been provided. These pupils are allowed to bring mobile phones to school (to enhance their safety during their journey to/from school), but these devices are to be given to the class teacher for safekeeping throughout the school day. **They must not be used on the school site at any time.**

If pupils breach these roles, the Headteacher will be informed and normal disciplinary procedures will be followed.

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 powers included in the Education Act only extend to devices in the possession of pupils – they do not extend to devices owned (or mislaid) by other parties e.g. a visiting parent or contractor).

The authorised member of staff should take care that, where possible, searches should not take place in public places (e.g. an occupied classroom), which might be considered as exploiting the 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) who, if at all possible, should also 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 they reasonably believe that 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.

Extent of the search
The person conducting the search may not require the pupil to remove any clothing other than outer clothing (clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear – outer clothing includes hats, 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.

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the flow chart within the section Responding to Incidents of Misuse.

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

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. Advice should be sought from the Headteacher for further guidance if required.

A record should be kept of the reasons for the deletion of data / files.

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.

Audit / Monitoring / Reporting / Review
The 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, using the log sheet (see Appendices).

These records will be reviewed by the Safeguarding Governor on an annual basis.

This policy will be reviewed by the Headteacher and Governors every three years and in response to changes in guidance and evidence gained from the records.

LEGISLATION

The school community should be aware of the legislative framework within which the Online Safety Policy template (on which this policy is based) was produced by SWGfL. 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.

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

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

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

The Data Protection Act 2018
Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

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

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.

Monitoring but not recording is also permissible in order to:

- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

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

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment 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 a 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.
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

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.

LINKS TO OTHER ORGANISATIONS AND DOCUMENTS

The following links may help in developing or reviewing the school e-safety policy.

UK Safer Internet Centre
Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/

CEOP
CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others
LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety
Netsmartz - http://www.netsmartz.org/

Tools for Schools
Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk
SWGfL Test filtering - http://testfiltering.com/
UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment
Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
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

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

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework