Audenshaw School

Acceptable Usage Policy

This policy is reviewed every two years by the Resource Committee.

History of Document

Issue No	Author/Owner	Date Written	Approved by Resource	Received by Governors	Comments
Issue 1	Steven Morton	29/03/2016	07/04/2016	07/04/2016	New policy following the implementation of new IT solution
Issue 2	Steven Morton	19/03/2018	23/04/2018	23/04/2018	Revised policy in order to comply with GDPR
Issue 2.1	Steven Morton	30/04/2020	14/05/2020	14/05/2020	Minor changes
Issue 2.2	Steven Morton	13/05/2021	10/06/2021	10/06/2021	Minor changes
Issue 2.3	Mark Wright	12/07/2022	01/12/2022	01/12/2022	Minor changes

OUR MISSION

Our school aims to provide a quality education in a caring community based on values of respect, responsibility and resilience and a relentless pursuit of excellence in all that we do.

OUR VISION

Our School will be recognised as a fully inclusive, aspirational, high achieving centre of excellence, firmly rooted in the local community.

We will create, develop and maintain a challenging and stimulating personalised learning environment where no student is overlooked or left behind and where teaching and learning is high quality, inspirational and innovative.

We will consistently have high academic standards and expectations for every individual and continue to place considerable value on sport and healthy living and developing strong links with the community.

All members of our school community will be valued and every success will be celebrated.

Our School will maintain a safe, secure and caring environment in which to work and learn.

AUDENSHAW SCHOOL SAFEGUARDING STATEMENT

This School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

CONTENTS

This policy applies to all members of the school community (including staff, students, 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 Principals to such extent as is reasonable, to regulate the behaviour of students 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 cyber-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 for template 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 / carers of incidents of inappropriate e-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:

Principal and Senior Leadership

- The Principal/ 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 e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the IT Manager where/when concerns are raised via fastvue alerts..

IT Manager / Technical staff:

The IT Manager is 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
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis as soon as changes are made (daily/instant)
- that they keep up to date with e-safety technical information in order to effectively carry out their role and to inform and update others as relevant
- that the use of the network / remote access desktops & applications / school email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal for investigation.
- that monitoring software / systems are implemented and updated.

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 Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Principal for investigation.
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems and where images/video is used, this should be logged in the Information Asset Register
- students understand and follow acceptable use policies
- students 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 students 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

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
- cyber-bullying

Students

- **are responsible for using the school digital technology systems in accordance with the Student 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 other electronic devises. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the *school's* Acceptable Use Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.*

Parents and carers 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

- access to parents' sections of the website / VLE and on-line student records including the details available and editable within the SIMS Parent App and keeping the records held in respect of the students and themselves up to date
- their children's personal devices in the school (where this is allowed)

Policy Statements

Education – students
Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students 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.

E-safety should be a focus in all areas of the curriculum and 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 should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- students 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
- students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- students should be helped to understand the need for the student 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 students 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 students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Manager (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.

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 above sections will be effective in carrying out their e-safety responsibilities:

- school technical systems will be managed in ways that ensure that the school meets recommended Government & 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
- 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. Users are responsible for the security of their username and password *and will be required to change their password every 90 days*
- the "administrator" passwords for the school ICT systems, used by the IT Manager/Technician must also be available to the Principal or other nominated senior leader and kept in a secure place (e.g. school safe)
- the IT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband and filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- the school has provided enhanced / differentiated user-level filtering as well as proactive reporting on inappropriate use of the Internet and school systems
- 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.
- an appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person. In the first instance for students this will be your form teacher.
  Staff should report any loss of data (regardless of format, e.g digital files, loss of laptop, loss of USB stick, data recorded on paper or any other breach that can be considered a loss of data to the Principal, DPO and IT Manager immediately
- 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
- a policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. Any request for such access should be made through the HR department initially
- an agreed policy is in place within the relevant Acceptable Use appendices, regarding the extent of personal use that users (staff / students) and their family members are allowed on school devices that may be used out of school
- a network policy is in place that prevents staff from downloading executable files and installing programs on school devices. USB devices in all forms are prohibited and restricted from being used on school devices
- personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Access to VDI sessions on http://vdi.audenshawschool.org.uk is categorised as onsite usage.

Use of digital and video images

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

educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- when using digital images, staff should inform and educate students 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 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 students 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
- Staff are responsible for ensuring before ANY image or video is used on the school website, any third party website, app or social media/marketing outlet, that the appropriate consent is in place from the parent/carer and where a student is over 13, that consent is also obtained from the student. In order to comply in the event of consent being withdrawn, the details within the Information Asset Register must be updated.
- care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- students must not take, use, share, publish or distribute images of others without their permission
- photographs/video published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images
- students' full names will not be used ANYWHERE on a website or blog, particularly in association with photographs. Where the context benefits from discreet non-personal identifiers these details should be anonymised to first name or initials
- written permission from parents or carers will be obtained before photographs of students are published on the school website or on any social media/marketing materials etc. Students over 13 will be required to give specific personal consent also. It should be noted that under new data protection rules (GDPR) consent can be withdrawn at any time and therefore it is vital staff record the details of this within the Information Asset Register
- student's work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the UK General Data Protection Regulation 2018 which states that personal data (any information relating to an identified or identifiable natural person, data subject) must be:

- Fairly and lawfully processed
- Processed for specified purposes as detailed in school privacy notice
- 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 and not outside the European

Economic Area (EEA)

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"
- it has a Data Protection Policy
- it is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- 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
- data subjects have the right to erasure (also known as the right to be forgotten) where data is no longer necessary in relation to the purpose for which it was originally collected or when the individual withdraws consent in relation to any data collected for which consent was 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.

Staff must ensure that they:

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

Personal data should only be stored on school owned network systems. Any exported data must have the consent of the Principal and the data must be encrypted and password protected

- the device must be password protected (please note that many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete
- the school recommendation is that staff/students wishing to access any school systems to do so via the virtualised remote desktop access on which access is securely controlled and data remains on the school site.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these

technologies for education outweighs their risks / disadvantages:

	Staff & other adults			Students				
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	X			X				
Use of mobile phones in lessons		X		X				
Use of mobile phones in social time	X			X				
Taking photos on mobile phones / cameras	X			X				
Use of other mobile devices e.g. tablets, gaming devices	X			X				
Use of personal email addresses in school, or on school network		X		X				
Use of school email for personal emails		X					X	
Use of messaging apps (MS Teams)	X						X	
Use of social media	X			X				
Use of blogs	X			X				

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

- ensure adherence with the School Email Policy
- users must immediately report, to their line manager/form teacher – 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
  students or parents / carers (email, chat, MS Teams 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.
- students 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

All schools, academies and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, 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 students, staff and the school through limiting access to personal information:

- training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
- specific training on the new GDPR data protection regulations
- 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 students, 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
- 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 IT Manager and Senior Leadership Team to ensure compliance with this policy and schools values.

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 as well as their own personal devices. The school policy restricts usage as follows:

User Actions		Acceptable if personaldata anonymised	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	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

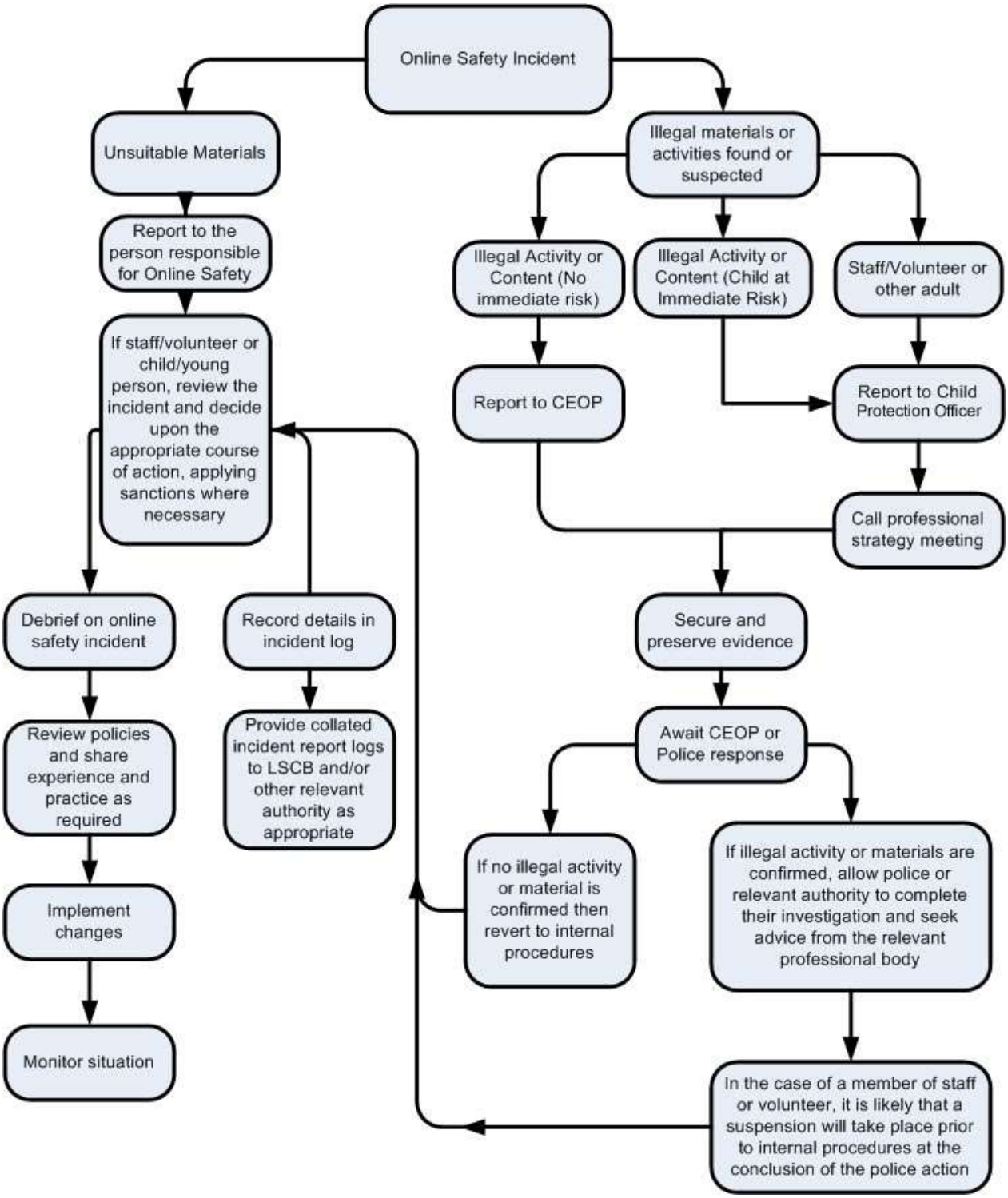
pass on, material, remarks, proposals or comments that contain or relate to:	**Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986**					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	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	
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 (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce				X		
File sharing	X					
Use of social media				X		
Use of messaging apps				X		
Use of video broadcasting eg Youtube				X		

Responding to incidents of misuse

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

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the Designated Safeguarding Lead and Principal who will report 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 Designated Safeguarding Lead and Principal who will then refer to the Police. 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
    - 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 *(Being Referred to Assistant Principal (Behaviour & Attitudes & Principal respectively) consideration to be given by the reviewer of this policy as to whether or not we refer to behaviour/disciplinary policies or use the tables below for students and staff to specify for the purposes of this acceptable use policy the actions and consequences for a breach under each category. What is clear is we will have much greater access to the data that will dramatically increase the probability of breaches being identified and in my opinion we should therefore be very clear what is and what isn't acceptable. A key example of this to me is the use of proxy avoidance sites to bypass the filtering we have in place. This is one of the most serious breaches we can have and how we deal with this is paramount to the efficacy of internet filtering.*

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:

Students — Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to 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		X	
Unauthorised use of non-educational sites during lessons	X				X	X		X	
Unauthorised use of mobile phone / digital camera / other mobile device	X					X		X	
Unauthorised use of social media / messaging apps / personal email	X					X		X	
Unauthorised downloading or uploading of files	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 student'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		X
Corrupting or destroying the data of other users		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	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 / academy's filtering system	X	X				X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	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

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Principal Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical 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								
Unauthorised downloading or uploading of files								
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								
Careless use of personal data eg holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature								
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school								
Using proxy sites or other means to subvert the school's / academy's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material								
Breaching copyright or licensing regulations								
Continued infringements of the above, following previous warnings or sanctions								

Digital technologies have become integral to the lives of children and young people, both within school 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 *students* will have good access to digital technologies to enhance their learning and will, in return, expect the *students* 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 will only use ICT in school for school purposes.
- I will only use my school email address when sending an email.
- I will only open email attachments from **people I know, or who my teacher has approved.**
- I will not tell other people my ICT passwords.
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my e-Safety.
- I understand I must not do anything that would damage Audenshaw School's reputation, my family and friends' reputation or my own reputation.
- I will not use the Internet for personal financial gain, gambling, political purposes or advertising.

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 or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, or video broadcasting (e.g. YouTube).

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 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 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 damage or faults involving equipment or software, however this may have happened.

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs)
- I will not install or attempt to install or store programs of any type on any school device, nor will I try to alter computer settings.
- I will NOT access or use social media sites using any school systems

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, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

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

Student Acceptable Use Agreement Form
This form relates to the *student* Acceptable Use Agreement, to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:
- I use the *school* systems and devices (both in and out of school)
- I use my own devices in the *school* (when allowed) e.g. mobile phones, gaming devices, USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, accessing school email, website etc.

Name of Student	
Group / Class	
Signed	
Date	

Use of Digital / Video Images

Images may also be used to celebrate success through their publication in newsletters, on the school

website and occasionally in the public media. In the event of being used for marketing material for the school, a separate consent will be requested and will detail the length of time this material will be used and you will be consenting to its use for that period only. Consent in these circumstances can only be withdrawn if this is reasonably possible to do. In the event of a school prospectus having been distributed for example, it would be unreasonable to expect the school to remove these in any level of entirety within the public domain.

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 (e.g. not using full 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 *students* in the digital / video images.

Parents / carers and students over 13 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 Consent Form

Parent / Carer's Name	
Student Name	

As the parent / carer of the above *student*, 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

Parent Signature	
Student Signature	
Date	

Use of Cloud Systems Permission Form

The school uses Microsoft Office 365 for the Education of students and staff. This permission form describes the tools and student responsibilities for using these services.

The following services are available to each student and hosted by Microsoft. They are integrated into the school systems

Mail - an individual email account for school, use of which is managed by the school

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

Office Suite - a word processing, spreadsheet, drawing, and presentation toolset

Sites - an individual and collaborative website creation tool

Using these tools, student's collaboratively create, edit and share files and websites for school related projects and communicate via email with other students and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student 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 Microsoft terms and conditions we are required to seek your permission for your child to have a Microsoft Office 365 for Education account:

Parent / Carer's Name	
Student Name	

As the parent / carer of the above student I agree to my child using the school using Microsoft Office 365 for Education.	Yes / No

This is a onetime consent and any withdrawal of consent once an account is created lies within the responsibility of yourself to communicate this with Microsoft directly.

Signed	
Date	

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 / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can generate 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 ICT 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 ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *student* 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 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. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities gained from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:
- I understand that the *school* will monitor my use of the ICT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT 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 laid out 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 for someone to 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* ICT 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) 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 students 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 has 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 ICT systems unless previously agreed by a member of SLT
- 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 programs)
- 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, adult pornography covered by the Obscene Publications Act), 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 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, 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 Data Protection 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 student 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*:

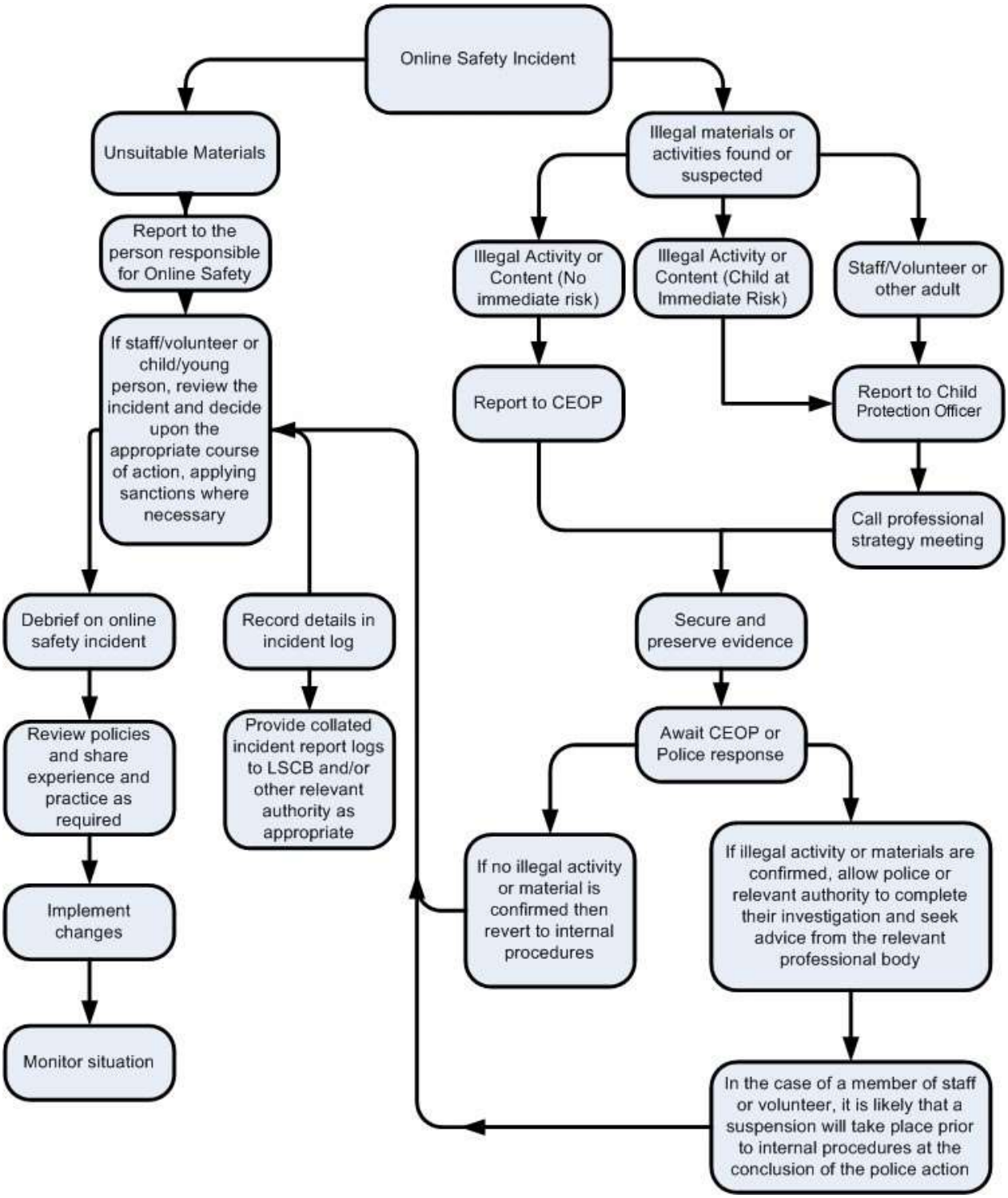
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- 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 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.

Staff / Volunteer Name	
Signed	
Date	

Responding to incidents of misuse – flow chart



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

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

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

Web site(s) address / device Reason for concern

Conclusion and Action proposed or taken

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, along with 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 a right to 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 their actions while connected to the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities
The management of technical security will be the responsibility of the IT 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 academy 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 systems
- users will be made responsible for the security of their username and password. They must not allow other users to access the school systems using their log on credentials and must immediately report any suspicion, or evidence that there has been a breach of security
- the IT Manager 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
- 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 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 programs on school devices by users
- an agreed policy is in place regarding the extent of personal use that users (staff / students / community) 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 and email.

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 (or other person) and will be reviewed, at least annually, by the E-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 Principal or other nominated senior leader and kept in a secure place e.g. school safe.
- passwords for new users, and replacement passwords for existing users will be allocated by the IT Support team. All teachers have the ability to change/reset student passwords
- all users (adults and young people) will have responsibility for the security of their username and password. They 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 student sections below
- 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.

Staff passwords:

- all staff users will be provided with a username and password by the IT Manager who will keep an up to date record of users and their usernames
- the password should be a minimum of 8 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. This will ensure that other systems are not put at risk if one is compromised.
- users should ensure that passwords they use for school systems are different to the ones they use for non-school related systems (personal e-mail, social media etc.)
- should be changed at least every 60 to 90 days
- significantly different from previous 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.

Student passwords

- all students will be provided with a username and password by their IT teacher
- users will be required to change their password every term
- students will be taught the importance of password security
- the complexity (i.e. minimum standards) will be set in line with standard practice in a bid to ensure students go into life beyond school with an understanding that secure passwords

should be normal practice. This is a move away from the current philosophy of very simple or non-existing passwords and this will lead to an increase in access issues while younger students in particular adapt.

Training / Awareness

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

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

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

- in IT lessons
- through the Acceptable Use Agreement.

Audit / Monitoring / Reporting / Review

The IT Manager will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- 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 e-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 IT Manager. 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 the e-safety co-ordinator.

All users have a responsibility to report immediately to the IT Manager, 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 programs 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 Dell (Nviron)
- The school has provided enhanced / differentiated user-level filtering through the use of the Sonicwall filtering programme. (allowing different filtering levels for different ages / stages and different groups of users – staff / students etc)
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal.
- 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 IT Manager
- Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager (If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Group).

Education / Training / Awareness
Students will be made aware of the importance of filtering systems through e-safety education. 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

School Personal Data Handling Policy

Introduction
Schools and their employees should do everything within their power to ensure the safety and security of any material that is of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data to ensure that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in the relevant data protection legislation and relevant regulations guidance.

Policy Statements

The school 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 Data Protection Policy

Personal Data
The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

Personal information about members of the school community – including students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records

Curricular / academic data e.g. class lists, student progress records, reports, references

Professional records e.g. employment history, taxation and national insurance records, appraisal records and references

Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Registration
The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Training & awareness
All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners.

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

All users will use strong passwords which must be changed regularly. User passwords must never be shared.

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

All storage media must be stored in an appropriately secure and safe environment that avoids physical

risk, loss or electronic degradation.

Personal data can only be stored on school owned devices (this includes computers and portable storage media. Private equipment (ie owned by the users) must not be used for the storage of personal data.

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

- the export of data should have specific approval from the Principal
- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

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

The school has a clear policy and procedures for the use of "Cloud Based Storage Systems" and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The *school* recognises that under Section 7 of the DPA data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted, password protected and transported securely for storage in a secure location
- Users must take particular care to ensure that computers or removable devices which contain personal data cannot be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they

should preferably have secure remote access to the management information system or learning platform;

- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if they have specific permission to do so by the Principal and the storage media, portable or mobile device is encrypted and transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.

Disposal of data
The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

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

A log will be kept of all data that is disposed of to include the document ID, classification, date of destruction, method and authorisation.

School Policy: Electronic Devices - Searching & Deletion

Introduction

The changing face of information technologies and ever increasing student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search students 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 Principal (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 *Principal* must publicise the school behaviour policy, in writing, to staff, parents / carers and students at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

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

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.

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

If students breach these roles:

The sanctions for breaking these rules can be found in the Mobile Phone and Behaviour Policy

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

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

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a student 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 e.g. an occupied classroom, which might be considered as exploiting the student being searched.

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

There is a limited exception to this rule: authorised staff can carry out a search of a *student* of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

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

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

'Possessions' means any goods over which the *student* has or appears to have control – this includes desks, lockers and bags

A student's possessions can only be searched in the presence of the student 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.

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.

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.

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.

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.

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse.
CPC	Child Protection Committee
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
GDPR	General Data Protection Regulation
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
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 to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
TUK	Think U Know – educational e-safety programs for schools, young people and parents.

VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol