

Online Safety School Policy

Reviewed by:	Pupil Development, Wellbeing & Safety Committee
Signed (Governing Board):	
Date:	February 2017
Next Review due:	February 2020

Produced by Turton School

Development / Monitoring / Review of this Policy

This Online policy has been developed by a working group made up of:

- Head Teacher and Deputy Head Teachers
- Safeguarding Lead, Computing Subject lead
- ICT Network Manager
- Associate Assistant Head, Pastoral
- Business Manager

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

Schedule for Development / Monitoring / Review

This Online policy was approved by the <i>Governing Board</i> on:	23 rd January 2017
The implementation of this Online policy will be monitored by the:	Teaching, Learning and Curriculum Committee
Monitoring will take place at regular intervals:	Once a year
The <i>Governing Board</i> will receive a report on the implementation of the Online policy generated by the monitoring group (which will include anonymous details of Online incidents) at regular intervals:	At least once a year
The Online Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online or incidents that have taken place. The next anticipated review date will be:	November 2017
Should serious Online incidents take place, the following external persons / agencies should be informed:	LADO, police, Child Protection Officer

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys of students, parents and staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online 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. 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 behaviour that take place out of school.

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy. This will be carried out by the Teaching and Learning Sub Committee receiving regular information about online incidents and monitoring reports. A member of the Governing Board has taken on the role of Safeguarding governor and will include monitoring of this policy.

Head teacher and Senior Leaders:

- The Head teacher has a duty of care for ensuring the safety (including Online) of members of the school community, though the day to day responsibility for Online will be delegated to the deputy heads.
- The Head teacher and deputy heads are aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff. (See flow chart on dealing with Online incidents – included in a later section – “Responding to incidents of misuse” and relevant School disciplinary procedures).
- The Head teacher and Senior Leaders are responsible for ensuring that the relevant staff receive suitable training to enable them to carry out their Online roles and to train other colleagues, as relevant.
- The Head teacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online 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.

Online Safety subject leader:

- takes day to day responsibility for Online issues and has a leading role in establishing and Reviewing the school online policies
- ensures that all staff are aware of the procedures that need to be followed in the event of an online incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online incidents and creates a log of incidents to inform future Online developments,

- meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant Sub-committee of Governors
- reports regularly to Senior Leadership Team

Network Manager

The Network 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 online technical requirements and any Local Authority Online Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online technical information in order to effectively carry out their Online role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher for investigation and relevant action
- that monitoring software / systems are implemented, and updated annually.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online matters and of the current school Online policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Head Teacher and relevant action sanction
- all digital communications with students and parents should be on a professional level and only carried out using official school systems
- Online issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online and 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.

At least one of the Designated Child Protection Officers

should be trained in Online 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.

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

- the monitoring of the school online policy
- the monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents and the students about the online provision
- monitoring improvement actions identified through use of safe self-review tool.

Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable User Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online practice when using digital technologies out of school and realise that the school's Online Policy covers their actions out of school, if related to their membership of the school
- 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 parents' evenings, newsletters, letters, website / VLE and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online 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
 - their children's personal devices in the school

Community Users

Community Users who access school systems / website / VLE 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 the Community Users Acceptable Use Policy.)

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

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

- A planned online safety curriculum should be provided as part of Computing and should be regularly revisited
- Key Online 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 Policy (AUPs) 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, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents

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

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

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents evenings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g.

www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers> (See appendix for further links / resources.)

Education – The Wider Community

The school will provide opportunities for members of the community to gain from the school's online safety knowledge and experience.

Online messages targeted towards grandparents and other relatives as well as parents. The school website will provide online information for the wider community.

Education & Training – Staff / Volunteers

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

- A planned programme of formal and informal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
- Safeguarding and Computing lead or other nominated person will receive regular updates through attendance at external training events (e.g. from / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online safety policy and its updates will be presented to and discussed by staff meetings.
- Safeguarding and Computing lead will provide advice, guidance and training to individuals as required.

Training – Governors

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

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

Technical – infrastructure / equipment, filtering and monitoring

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- All users will be provided with a username and secure password by the ICT Technical Team who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every year
- The “administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)

- T Kwiatkowski, Network 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 or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- The school has provided differentiated user-level filtering for KS3 and 4, Sixth Form and staff
- 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; report to Network Manager or Curriculum Deputy Head Teacher, for users to report any actual / potential technical incident / security breach to the relevant person
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software
- An agreed policy is in place for the provision of temporary access of “guests” - trainee teachers and supply teachers are treated as staff for the period they are here and onto the school systems
- Guest account with limited accessibility and permission levels set up as needed. Requests must be made to technical staff and their family members are allowed on school devices that may be used out of school. Use can be monitored and devices must be regularly returned to school (at least termly) for software updates to occur

Staff are unable to download executable files and install the programmes on school devices.

The use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices is allowed. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (See School Personal Data Policy in the appendix for further detail).

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. ([See appendix for BYOD Policy.](#))

The school has a set of clear expectations and responsibilities for all users

The school adheres to the Data Protection Act principles

All users are provided with and accept the Acceptable Use Agreement

All network systems are secure and access for users is differentiated

Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises

All users will use their username and password and keep this safe

Students receive training and guidance on the use of personal devices

Regular audits and monitoring of usage will take place to ensure compliance

Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy

Any user leaving the school will follow the process outlined within the BYOD policy.

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 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 are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents 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.
- 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. Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Photographs 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.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

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

The school will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". ([See Privacy Notice section in the appendix.](#))
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Senior Information Risk Officer (SIRO) and Business Manager will carry out risk assessments to ensure there are clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

Staff must ensure that they:

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

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

- the data must be encrypted and password protected
- the device must be password protected (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.

See the Personal Data Handling Policy Template in the appendix provides more detailed guidance on the school's responsibilities.

Communications

	Staff & other adults				Students			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to school	✓				✓			
Use of mobile phones in lessons							✓	
Use of mobile phones in social time	✓				✓			
Taking photos on persmobile phones / cameras		✓					✓	
Use of other mobile devices e.g. tablets, gaming devices				✓				✓
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails		✓					✓	
Use of messaging apps		✓						✓
Use of social media			✓					✓
Use of blogs		✓					✓	

This is an area of rapidly developing technologies and uses. Turton School allows students to use mobile phones in lesson at the request of the teacher only. Sixth form students may use phones as long as they do not disturb the learning in lessons.

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 disadvantages:

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and students or parents (email, chat, VLE 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 will be provided with individual school email addresses for educational use.
- Students should be taught about Online 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

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's Online framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools, academies 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, 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 pupils, 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.
- 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 or school staff
- They do not engage in online discussion on personal matters relating to members of the school community personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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

Unsuitable / inappropriate activities

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

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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 (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	

Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce		X			
File sharing		X			
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. YouTube		X			

Responding to incidents of misuse

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

Illegal Incidents

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

Other Incidents

It is hoped that all members of the 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 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 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 other criminal conduct, activity or materials. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School Actions & Sanctions

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

Students

Actions / Sanctions

Incidents:	Refer to child protection lead	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Head teacher /	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X		X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons		X				X	X	X	X	X
Unauthorised use of mobile phone / digital camera / other mobile device		X					X	X	X	X
Unauthorised use of social media / messaging apps / personal email		X				X	X	X	X	X
Unauthorised downloading or uploading of files		X				X	X	X	X	X
Allowing others to access school network by sharing username and passwords		X					X	X		
Attempting to access or accessing the school network, using another student's account								X	X	
Attempting to access or accessing the school network, using the account of a member of staff			X	X		X	X	X		
Corrupting or destroying the data of other users			X	X		X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X		X			X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions				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		
Using proxy sites or other means to subvert the school'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 manager	Refer to Head teacher	Refer to Local Authority Designated Officer & HR	Refer to Police	Refer to Technical Support Staff for action	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		X	X	X
Inappropriate personal use of the internet / social media / 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 or attempting to access or accessing the school network, using another person's account	X				X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X				X		
Deliberate actions to breach data protection or network security rules	X	X				X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students	X	X				X	X	X
Actions which could compromise the staff member's professional standing		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	X
Using proxy sites or other means to subvert the school's filtering system		X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X				X	X	X
Deliberately accessing or trying to access offensive or pornographic material		X			X	X	X	X
Breaching copyright or licensing regulations	X				X	X		
Continued infringements of the above, following previous warnings or sanctions		X					X	X

Appendix

Acknowledgements

Bolton Safeguarding in Education Team and the Online Safety Group would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Policy Template:

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

Appendices

Can be found on the following pages:

- Student Acceptable Use Agreement template (secondary setting)
- Staff and Volunteers Acceptable Use Agreement Policy template
- Community Users Acceptable Use Agreement
- Responding to incidents of misuse – flowchart
- Record of reviewing sites (for internet misuse)
- School Reporting Log template
- School Online Safety Audit Checklist template
- School Technical Security Policy template
- School Personal Data Policy template
- School Policy Electronic Devices, Search and Deletion
- School Bring Your Own Devices (BYOD) Policy
- School Online Committee Terms of Reference
- Legislation
- Links to other organisations and documents
- Glossary of terms

Student Acceptable Use Policy

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe 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 understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, general educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

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

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

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

- I will not take or distribute images of anyone without their permission.

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

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

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.

By accessing the school network I confirm that I have read, understood and agree to the rules involved in this acceptable use agreement.

Use of Digital / Video Images

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

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

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

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

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

Digital / Video Images Permission Form

Parent Name

Student Name

As the parent 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.

Signed

Yes / No

Date

Staff (and Volunteer) Acceptable Use Policy Agreement

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 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 students 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 to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online 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 set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of to the appropriate person
- I will be professional in my communications and actions when using school 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 image
- I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students and parents using official school. System such communication will be professional in tone and manner. I am aware of the risks attached to using my personal email addresses / mobile phones / social networking sites for such communications.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use.
- I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will 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) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, without permission from the network manager or SLT.
- 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 Personal Data 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. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

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

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

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

Acceptable Use Agreement

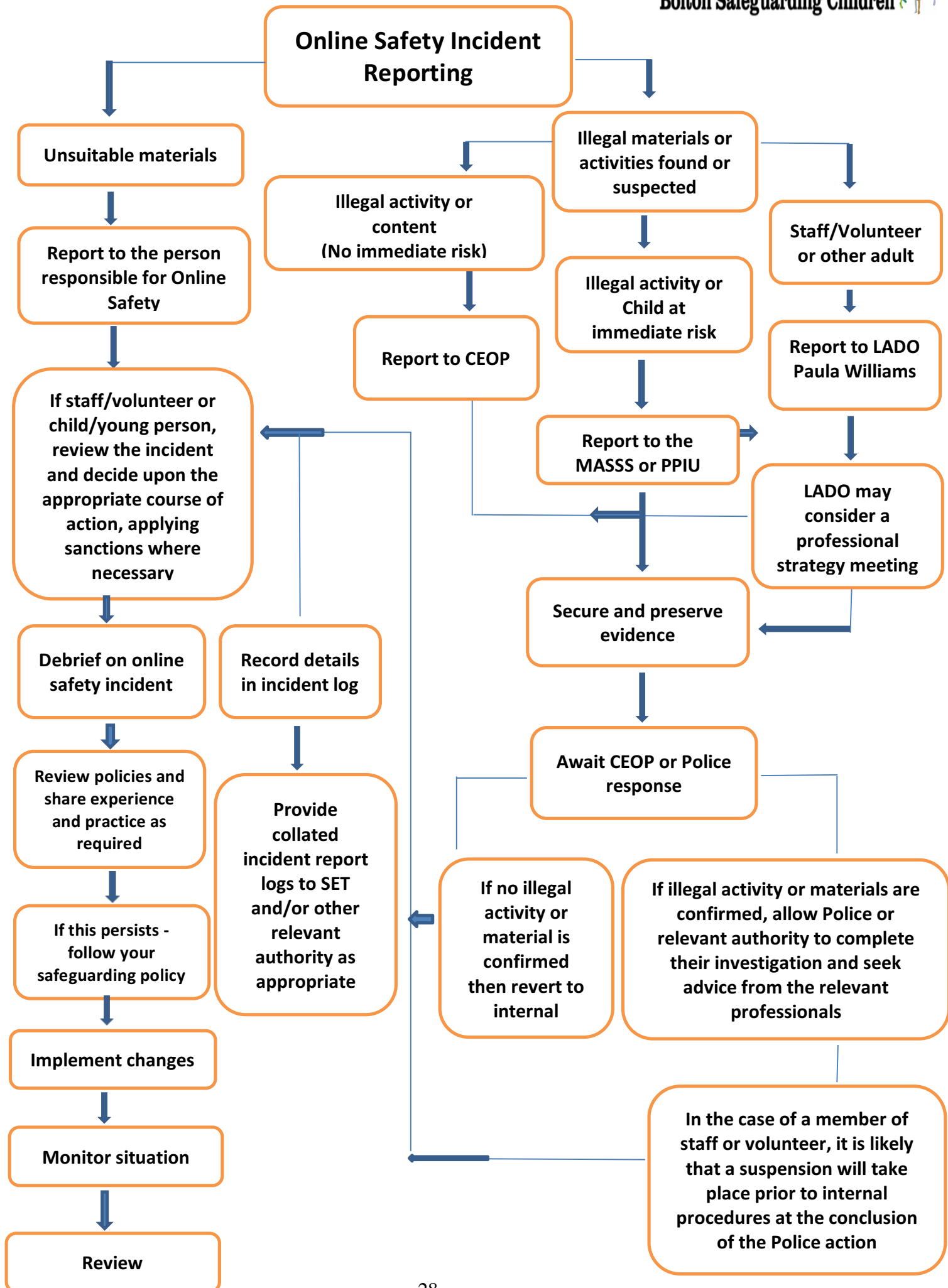
I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school

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

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

Print Name / Signature

Date



Support Contacts for Bolton Schools

SET – Safeguarding in Education Team:

- Jacqui Parkinson – Safeguarding in Education Officer – 01204 337472
- Natalie France – Safeguarding Education Social Worker – 01204 331314

LADO: Paula Williams - 01204 337474

Bolton's MASSS – 01204 331500

Police protection investigation unit – 0161 856 7949

Community Police - 101

EXIT Team – 01204 337195

Bolton Safeguarding Children's Board: Shona Green – 01204 337964

If there is an ICT network issues contact the school ICT technicians on 222.

If your provider is Bolton School ICT Unit – contact 01204 332034 or

contact@sict.bolton.gov.uk

ONLINE INCIDENT LOG

Details of ALL Online incidents to be recorded by the staff on CPOMS.

Online Safety Audit Checklist

This quick self-audit will help the senior leadership team assess whether the online safety basics are in place.

Has the school an Online Safety Policy that complies the latest guidance?	
Date of latest review:	
The Policy was agreed by governors on :	
The Policy is available for staff at:	
And for parents at:	
The Designated Safeguarding lead is:	
The Online Safety / Computing lead is:	
Has Online Safety training been provided for staff?	
Has Online Safety training been provided for pupils?	
Do parents sign & return - An agreement that their child will comply with the School Online Safety - The Acceptable User Policy (AUP) for pupils ? - An agreement that their children's work & pictures may be displayed on the internet.	
Has the school got an AUP / Online Safety Rules age appropriate for pupils?	
Is the AUP / Online Safety rules displayed in all rooms with computers?	
Internet access is provided by an educational Internet service provider and complies with DfES requirements for safe and secure access?	
Has an ICT security audit been initiated by SMT, possibly using external expert?	
Is personal data collected, stored and used according to the principles of Data Protection Act?	

Members of our school that have had inputted directly with this policy	
Head Teacher	SG
Member of Senior Leadership Team	CEB
Online Safety / Computing lead	AMB
Designated Safeguarding lead	UMH
Linked Governor	J Harte

School Technical Security Policy (including filtering and passwords)

Introduction

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

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

Responsibilities

The management of technical security will be the responsibility of T Kwaitowski, Network Manager.

Technical Security

Policy statements

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the SLT.

- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The Network 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. Students and staff can access the wireless network using their school username and password to do so.
- 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
- Staff can use the ICT helpline or email to report any technical incident to the Network Manager.
- The agreed provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school system is trainee and supply teachers will be treated as staff members for the duration of their time at Turton. Guest accounts can be activated on a needs basis in consultation with the Network Manager.
- Staff cannot download executable files and install programmes on school devices. This must only be done by ICT technical staff.
- It is agreed that staff can use school devices for legal personal activities and their family members are allowed on school devices that may be used out of school, but family members cannot remote access the School network.
- School Network: The use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices is allowed. Any personal data must be password protected. ([See School Personal Data Policy in the appendix for further detail.](#))
- 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. ([See School Personal Data Policy in the appendix for further detail.](#))

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

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 SLT.

- **All school networks and systems will be protected by secure passwords that are regularly changed**
- **The “master / administrator” passwords for the school systems, used by the technical staff must also be available to the Headteacher 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 ICT Technical Team.
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Users will change their passwords on a yearly basis

Staff passwords:

All staff users will be provided with a username and password by the network manager who will keep an up to date record of users and their usernames.

- must not include proper names or any other personal information about the user that might be known by others
- the account should be “locked out” following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- should be changed on a yearly basis
- 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 users will be provided with a username and password** by ICT Technical Team who will keep an up to date record of users and their usernames.
- Users will be required to change their password every year.
- Students will be taught the importance of password security

Training / Awareness

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

- at induction
- through the school’s online policy and password security policy
- through the Acceptable Use Agreement

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

- in computing lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person (Deputy Head Curriculum) 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 online 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 Network 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 and authorised by a second responsible person** (Network Manager) *prior to changes being made*

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

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

Policy Statements

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

- The school maintains and supports the managed filtering service provided by the Internet Service Provider
- The school has provided enhanced / differentiated user-level filtering through the use of the Sophos Unified Threat Management Filtering Programme (allowing different

filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.).

- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head Teacher or Deputy Head Curriculum.
- 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 filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff in consultation with Deputy Head Curriculum.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the online education programme through assembly, tutorials and compulsory lessons. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- *the Acceptable Use Agreement*
- *induction training*
- *staff meetings, briefings, Inset.*

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online awareness sessions / newsletter /website.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Deputy Head Curriculum who will decide whether to make school level changes (as above).

Monitoring

Some schools supplement their filtering systems with additional monitoring systems. If this is the case, schools should include information in this section, including – if they wish – details of internal or commercial systems that are in use. They should also ensure that users are informed that monitoring systems are in place.

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Policy and the Acceptable Use Agreement.

Audit / Reporting

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

- the second responsible person, the Deputy Head Curriculum
- SLT on request
- Online Governor / Governors committee/Trustee
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

School Personal Data Handling Policy

School Personal Data Handling Policy

Recent publicity about data breaches suffered by organisations and individuals has made the area of personal data protection compliance a current and high profile issue for schools and other organisations. It is important that the school has a clear and well understood personal data handling policy in order to avoid or at least minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on your systems, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure.

In addition:

- No school or individual would want to be the cause of any data breach, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation.
- Schools are “data rich” and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- The school will want to avoid the criticism and negative publicity that could be generated by any personal data breach.
- The school is subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation.

It is a statutory requirement for all schools to have a Data Protection Policy:

<http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools>

Schools have always held personal data on the pupils in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations. Legislation covering the safe handling of this data is mainly the Data Protection Act 1998 (‘the DPA’). Moreover, following a number of losses of sensitive data, a report was published by the Cabinet Office in June 2008, Data Handling Procedures in Government. The latter stipulates the procedures that all departmental and public bodies should follow in order to maintain security of data. Given the personal and sensitive nature of much of the data held in schools, it is critical that they adopt these procedures too.

It is important to stress that the Personal Data Handling Policy applies to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall Online policy, this document will place particular emphasis on data which is held or transferred digitally.

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material 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 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 Officer 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 relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

The DPA lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The DPA requires organisations to comply with eight data protection principles, which, among others require data controllers to be open about how the personal data they collect is used.

The DPA defines “Personal Data” as data which relate to a living individual who can be identified (http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions)

from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It further defines “Sensitive Personal Data” as personal data consisting of information as to:

the racial or ethnic origin of the data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), his physical or mental health or condition, his sexual life, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Guidance for organisations processing personal data is available on the Information Commissioner’s Office website:

http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx

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 “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”. (See Privacy Notice section below.)

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 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 or by other agencies working with families or staff members.
- Responsibilities
- The school's Senior Information Risk Officer (SIRO) is the Business Manager. This person will keep up to date with current legislation and guidance and will:
- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)
- The school will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand :
 - what information is held, for how long and for what purpose,
 - how information has been amended or added to over time, and
 - who has access to protected data and why.

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

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

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

http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

Information to Parents– the “Privacy Notice”

In order to comply with the fair processing requirements of the DPA, the school will inform parents of all students of the data they collect, process and hold on the students, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom it may be passed. This privacy notice will be passed to parents through parents of young people who are new to the school will be provided with the privacy notice through the induction process and the website.

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

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

Recognising the risks that are present;

Judging the level of the risks (both the likelihood and consequences); and

Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
NOT PROTECTIVELY MARKED	0	Will apply in schools
PROTECT	1 or 2	
RESTRICTED	3	
CONFIDENTIAL	4	Will not apply in schools
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	

Most student or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, e.g. the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more

individual data elements together in a report or data view increases the impact of a breach. A breach that puts students at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. "Securely delete or shred this information when you have finished using it".

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, at least at yearly intervals. 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 equipment (this includes computers and portable storage media. Private equipment (i.e. 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 data must be encrypted and password protected,
- the device must be password protected
- the device must offer approved virus and malware checking software and
- 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 clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

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 R

estricted (or higher) material must be held in lockable storage, whether on or off site.

The *school* recognises that under Section 7 of the DPA, <http://www.legislation.gov.uk/ukpga/1998/29/section/7> 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, or transferred to the LA or other agencies. 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 and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.
-

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

Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident;

- a communications plan, including escalation procedures;_i
- and results in a plan of action for rapid resolution;_i and
- a plan of action of non-recurrence and further awareness raising.
- All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Use of technologies and Protective Marking

The following provides a useful guide:

	The information	The technology	Notes on Protect Markings (Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Privacy and Electronic Communications

Schools should be aware that the Privacy and Electronic Communications Regulations have changed and that they are subject to these changes in the operation of their websites.

Freedom of Information Act

All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests. In this policy the school should:

Delegate to the Headteacher day-to-day responsibility for FOIA policy and the provision of advice, guidance, publicity and interpretation of the school's policy.

Proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually.

Ensure that a well-managed records management and information system exists in order to comply with requests.

Ensure a record of refusals and reasons for refusals is kept, allowing the School to review its access policy on an annual basis.

Model Publication Scheme

The Information Commissioners Office provides schools with a model publication scheme which they should complete. This was revised in 2009, so any school with a scheme published prior to then should review this as a matter of urgency. The school's publication scheme should be reviewed annually.

Guidance on the model publication scheme can be found at:

http://www.ico.gov.uk/for_organisations/freedom_of_information/guide/publication_scheme.aspx

The Schools Model Publication Scheme Template is available from:

http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/schools_england_mps_final.pdf

Guidance and a Model Publication Scheme for Academies can be found at:

<http://www.education.gov.uk/schools/leadership/typesofschools/academies/open/a00205178/freedom-of-information-guide-for-academies>

Further Guidance

ICO guidance can be found at the following link - including a pdf version - updated in September 2012:

http://www.ico.gov.uk/for_organisations/freedom_of_information/guide.aspx

DfE guidance that is specific to Academies can be found at:

<http://www.education.gov.uk/aboutdfe/foi/disclosuresaboutschoools/a0076171/academies-and-freedom-of-information>

<http://www.education.gov.uk/schools/leadership/typesofschools/academies/open/a00205178/freedom-of-information-guide-for-academies>

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 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.

DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies"

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

Relevant legislation:

Education Act 1996

Education and Inspections Act 2006

Education Act 2011 Part 2 (Discipline)

The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012

Health and Safety at Work etc. Act 1974

Obscene Publications Act 1959

Children Act 1989

Human Rights Act 1998

Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfES 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 Head Teacher will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: Cathy Bach, Deputy and Ursula Hodgson, Deputy.

The *Head Teacher* has authorised members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices:

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

Training / Awareness

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

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

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

Members of staff authorised by the Head Teacher 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.

Students are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school. Students should not use phones in lessons, unless given permission by staff.

If students breach these rules the sanctions for breaking these rules can be found in the Behaviour Policy.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device

in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

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

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a student 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 do not extend to devices owned (or mislaid) by other parties e.g. a visiting parent or contractor, only to devices in the possession of students.

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

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**

Care should be taken not to delete material that might be required in a potential criminal investigation.

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

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the flow chart in the main School Template Policies document.

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. The staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

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

A record should be kept of the reasons for the deletion of data / files, using CPOMS to record the information.

Care of Confiscated Devices

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

Audit / Monitoring / Reporting / Review

The responsible person, Deputy Head (Pastoral), will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be kept on CPOMS.

This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance (DfE guidance will be reviewed in 2013) and evidence gained from the records.

School Bring Your Own Devices (BYOD) Pupil Policy

What does “bring your own device” mean?

Bring your own device (often shortened to BYOD) is the term used to describe the connection of a personally-owned device (such as a laptop, smartphone or tablet) to a Wi-Fi network provided by school.

Our school have decided to adopt this technology for the benefit of improving teaching and learning.

However this must be done in a safe and secure manner so the following rules have been put in place and must be followed by all users of this service.

Students may not use the devices to record, transmit or post photos or video of other teachers or students. No images or video recorded at school can be transmitted or posted at any time without the permission of their teachers.

Parent / pupil / users must request BYOD access and agree to the terms in this Acceptable User Policy (AUP)

Users must keep passwords secure and not share with non-registered users.

In the event of changing or losing a device registered for this service, the user must notify school so appropriate security measure can be taken.

When using a BYOD device, the user must adhere to all other AUPs regarding the safe use of the network, systems and internet.

The school has the discretion to allow and regulate the use of personal devices in the classroom and for use during specific projects.

Devices may not be used to cheat on assignments or tests or for non-instructional purposes (such as making a personal call and texting).

Mobile devices must be charged prior to bringing them to school so as to be usable during school hours. Charging devices in the school is not an option.

Liability

School does not take responsibility for lost, stolen, or damaged personal devices. Students are responsible for their digital property and should take appropriate measures to ensure any devices brought to school are secure throughout the school day. The school does not have the ability to electronically manage or filter a student's use of the Internet when he or she is connected via your wireless phone provider's 3G, 4G, or other data network connection.

Violations of Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges
- Notification to parents
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution

Legislation

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

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

Computer Misuse Act 1990

This Act makes it an offence to:

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

Data Protection Act 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.

Freedom of Information Act 2000

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

Communications Act 2003

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

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

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

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
 - Ascertain whether the communication is business or personal;
 - Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

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

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

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

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

Racial and Religious Hatred Act 2006

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

Protection from Harassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

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 Head teachers, 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.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Head teachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance)

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

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems
The School Information Regulations 2012

Requires schools to publish certain information on its website:

<http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestatoschoolinformationregulations>

Support for Bolton Schools

SET – Safeguarding in Education Team:

- Jacqui Parkinson – Safeguarding in Education Officer – 01204 337472
- Natalie France – Safeguarding Education Social Worker – 01204 331314

LADO: Paula Williams - 01204 337474

Bolton's MASSS – 01204 331500

Police protection investigation unit – 0161 856 7949

Community Police - 101

EXIT Team – 01204 337195

Bolton Safeguarding Children's Board: Shona Green – 01204 337964

If there is an ICT network issues contact your school ICT provider.

If your provider is Bolton School ICT Unit – contact 01024 332034 or contact@sict.bolton.gov.uk

Bolton Information Management Unit - Tasadiq.Naveed@bolton.gov.uk

<http://mossextranet.bolton.gov.uk/website/pages/DataProtectionandFreedomofInformation.aspx>

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy.

UK Safer Internet Centre

[Safer Internet Centre](#) -

[South West Grid for Learning](#)

[Childnet](#)

[Professionals Online Safety Helpline](#)

[Internet Watch Foundation](#)

CEOP

Public enquiries

Telephone: 0870 000 3344

For general enquiries or to verify a person as an NCA officer:

Email: communication@nca.x.gsi.gov.uk
Telephone: 0370 496 7622 (available 24/7)

<http://ceop.police.uk/ThinkUKnow>

Others:

INSAFE - <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis

Netsmartz <http://www.netsmartz.org/index.aspx>

Cyberbullying

[DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies](#)

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

Cyberbullying.org - <http://www.cyberbullying.org/>

Social Networking

Digizen – [Social Networking](#)

[SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people](#)

[Connectsafely Parents Guide to Facebook](#)

[Facebook Guide for Educators](#)

[https://www.disrespectnobody.co.uk/sexting/what-is-sexting/](https://www.disrespectnobody.co.uk sexting/what-is-sexting/)

Mobile Devices / BYOD

Cloudlearn Report [Effective practice for schools moving to end locking and blocking](#)

NEN - [Guidance Note - BYOD](#)

Data Protection

Information Commissioners Office:

[Your rights to your information – Resources for Schools - ICO](#)

[ICO pages for young people](#)

[Guide to Data Protection Act - Information Commissioners Office](#)

[Guide to the Freedom of Information Act - Information Commissioners Office](#)

[ICO guidance on the Freedom of Information Model Publication Scheme](#)

[ICO Freedom of Information Model Publication Scheme Template for schools \(England\)](#)

[ICO - Guidance we gave to schools - September 2012 \(England\)](#)

[ICO Guidance on Bring Your Own Device](#)

[ICO Guidance on Cloud Hosted Services](#)

[Information Commissioners Office good practice note on taking photos in schools](#)

[ICO Guidance Data Protection Practical Guide to IT Security](#)

[ICO – Think Privacy Toolkit](#)

[ICO – Personal Information Online – Code of Practice](#)

[ICO – Access Aware Toolkit](#)

[ICO Subject Access Code of Practice](#)

Bolton Information Management Unit - Tasadiq.Naveed@bolton.gov.uk

<http://mossextranet.bolton.gov.uk/website/pages/DataProtectionandFreedomofInformation.aspx>

Professional Standards / Staff Training

DfE - <http://www.rrrecruitment.com/wp-content/uploads/2016/04/Guidance-for-Safer-Working-Practice-October-2015.pdf>

Kent - [Safer Practice with Technology](#)

[Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs](#)

[Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs](#)

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

Working with parents and carers

[SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum](#)

[Connect Safely - a Parents Guide to Facebook](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[DirectGov - Internet Safety for parents](#)

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

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

[The Digital Universe of Your Children - animated videos for parents \(Insafe\)](#)

[Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide](#)

[Insafe - A guide for parents - education and the new media](#)

[The Cybersmile Foundation \(cyberbullying\) - advice for parents](#)

Research

[EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)

[Futurelab - "Digital participation - its not chalk and talk any more!"](#)

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
BSCB	Bolton Safeguarding Children’s Board
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
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
LADO	Local Authority Designated Officer
LAN	Local Area Network
MASSS	Multi-agency Screening and Safeguarding Service
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)
PPIU	Police Public Protection Investigation Unit
SET	Safeguarding in Education Team
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 programmes 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 Access Point

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in July 2016. However, BSCS cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal / professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.