George Fentham Endowed School

Online Safety Policy

(Version 4. Dec 2017)

Development / Monitoring / Review of this Policy

This online safety policy has been developed by a committee made up of:

- *Headteacher & Senior Leaders*
- *Online safety Lead*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors*
- *Parents and Carers*

Schedule for Development / Monitoring / Review

This online safety policy was approved by the *Board of Directors / Governing Body / Governors Sub Committee on:*	October 2017
The implementation of this online safety policy will be monitored by the:	*Online Safety Lead, Leadership & Management Team (to include Headteacher)*
Monitoring will take place at regular intervals:	*Termly*
The *Governing Body/ Governors Sub Committee* will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
The Online safety Policy will be reviewed in the Autumn Term, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	October 2018 (or as required)
Should serious online safety incidents take place, the following external persons / agencies will be consulted and, should the need arise, be more formally informed:	*Solihull ICT Manager, LA Safeguarding Officer, Police*

The school will monitor the impact of the policy using, as necessary:

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

Scope of the Policy

This policy applies to all members of the *school* community (including staff, students/ pupils, volunteers, parents/ carers, visitors, community users and Governors) 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 Headteachers to such extent as is reasonable, to regulate the behaviour of students/ pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour & Mobile Devices Policies.

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

Roles and Responsibilities

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

Governors:

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

The role of the Online Safety *Governor* includes, as appropriate:

- *on-going meetings with the Online Safety Lead*
- *on-going monitoring of online safety incident logs*
- *on-going monitoring of filtering/ change control logs*
- *reporting to relevant Governors/ Board/ committee/ meeting*

Headteacher and Senior Leaders:

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

Online Safety Lead:

At George Fentham Endowed School, the Online Safety Lead is Mr. S Bass, a member of the Leadership & Management Team.

- Leads the online safety committee
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/ documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority/ any relevant bodies
- Liaises with school technical staff (School Support Officer SSO)
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Meets regularly with Online safety *Governor* to discuss current issues, review incident logs and filtering logs
- Attends relevant meeting/ committee of *Governors (as appropriate)*
- Reports regularly to Senior Leadership Team

Network Manager/ Technical staff:

The *Network Manager/ Technical Staff/ Computing Lead* (We operate a 'Managed Network', monitored and maintained by Solihull LA/EICTS) are responsible for ensuring:

- that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack
- that the *school* meets required online safety technical requirements and any *Local Authority* Online Safety Policy/ Guidance that may apply (Solihull Managed)
- that users may only access the networks and devices through a properly enforced password protection policy
- *the filtering policy (managed and applied by Solihull LA), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person* (Solihull Managed)
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the *network/ internet/ Virtual Learning Environment/ remote access/ email* is regularly monitored in order that any misuse/ attempted misuse can be reported to the *Headteacher/ Senior Leader/ Online Safety Lead* for investigation/ action /sanction
- *that monitoring software/ systems are implemented and updated as agreed*

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current *school* online safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the *Headteacher/ Senior Leaders or Online Safety Lead* for investigation/ action/ sanction
- all digital communications with students/ pupils/ parents/ carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- students /pupils understand and follow the online safety and acceptable use policies
- students/ pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices (See separate Mobile Devices Policy)

- *in lessons where internet use is pre-planned students/ pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

Child Protection/ Safeguarding Designated Person (DSL)

The Designated Safeguarding Lead (DSL) & Deputy DSL are trained in online safety issues and be aware of the potential for serious child protection/ safeguarding issues to arise from:

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

Annual training for DSL (and 2 yearly for Deputy DSL) contains Online Safety elements which is always fed back to the Online Safety Lead and, subsequently, staff.

Online Safety Committee

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

Members of the *Online Safety Committee* will assist the *Online Safety Lead* with:

- the production/ review/ monitoring of the school online safety policy/ documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/ internet/ incident logs
- consulting stakeholders – including parents/ carers and the students/ pupils about the online safety provision (e.g. Year 2 INSPIRE Workshop).

Students/ pupils:

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

Parents/ Carers

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

- digital and video images taken at school events
- any information specific to parents' on the school website
- their children's personal devices in the school (At George Fentham this is only by prior agreement with the Headteacher)

Policy Statements

Education – students/ pupils

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

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum (Solihull Curriculum) is broad, relevant and provides progression, with opportunities for creative activities, and is augmented by the provision within the PSHE Curriculum (JIGSAW). It is provided in the following ways:

- a planned online safety curriculum is provided as part of Computing/ PHSE/ other lessons and is regularly revisited
- key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/ pastoral activities
- students/ pupils are taught, in all lessons, to be critically aware of the materials/ content they access on-line and are guided to validate the accuracy of information.
- students/ pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- *students/ pupils are helped to understand the need for the student/ pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school*
- *staff 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/ pupils are 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/ pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.*
- *it is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

Education – parents / carers

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

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

- *curriculum activities*
- *letters, newsletters, school website*
- *parents/ Carers sessions*
- *high profile events/ campaigns e.g. Safer Internet Day*
- *reference to the relevant web sites/ publications e.g.* www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

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

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

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 take place regularly, in the form of:

- a planned programme of formal online safety training will be made available to staff (either via internal CPD provision or external providers e.g; Solihull LA). This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly by the Online Safety Lead (S Bass).
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
- *the Online Safety Lead will receive regular updates through attendance at external training events (e.g. LA/ other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *this Online Safety policy and its updates will be presented to and discussed by staff in staff meetings/ on INSET days.*
- *the Online Safety Lead will provide advice/ guidance/ training to individuals as required.*

Training – Governors

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

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

Technical – infrastructure/ equipment, filtering and monitoring

The school has a managed ICT service provided by an outside contractor (Solihull LA), but it is still the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the *school* Online safety Policy/ Acceptable Use Agreements. The school should also check their Local Authority/ other relevant body policies on these technical issues.

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

- school technical systems will be managed in ways that ensure that the school / academy meets recommended technical requirements (these may be outlined in Local Authority / other relevant body policy and guidance)
- 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 Online Safety Lead, 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 encouraged to change their password regularly.*
- the "master/ administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Online Safety Lead and kept in a secure place.
- Online Safety Lead & SSO are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- internet access is filtered for all users. Illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list (Solihull

LA/EICTS monitor). Content lists are regularly updated and internet use is logged and regularly monitored.

- *the school has provided enhanced/ differentiated user-level filtering* (allowing different filtering levels for different groups of users – staff/ pupils /students etc)
- *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* (SSO Log on desktop/Inform Online Safety Lead) *for users to report any actual/ potential technical incident/ security breach to the relevant person, as agreed..*
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- an agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems (restricted login with no access to network drives).
- *an agreed policy is in place that does not allow staff to download executable files or install programmes on school devices (Restricted user access – only the administrators have this privilege).*
- *an agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

Bring Your Own Device (BYOD)

At George Fentham pupils, staff and visitors DO NOT use their own mobile devices during the school, unless in designated areas (Please see the separate Mobile Devices Policy). The educational opportunities offered by all other 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. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of online safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and our Mobile/Phone Devices Policy, along with the Acceptable Usage Policies, cover this in more detail (including BYOD).

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

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

Data Protection (Please also see the School's Data Protection Policy)

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.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. An appendix about School Personal Data is attached at the end of this document.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with Privacy Laws and lawfully processed in accordance with the associated "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed/ identified
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents

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

Communications

This is an area of rapidly developing technologies and uses.

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

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

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.
- users must immediately report, to the Online Safety Lead/Deputy DSL (Mr. S Bass), DSL (Mrs. A Edmeades) or Head (Mrs. J Gaughan) – 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/ pupils or parents/ carers (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.*
- *whole class/ group email addresses may be used at KS1, while students/ pupils at KS2 and above will be provided with individual school email addresses for educational use.*
- *students/ pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

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

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

- 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/ pupils, parents/ carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the *school* or local authority
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information (Privacy Settings).

The *school's* use of social media (Twitter feed) for professional purposes will be checked regularly (at least half termly) by the Online Safety Lead and Online Safety Committee (Pupil & Governor representatives) to ensure compliance with the appropriate aspects of the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

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

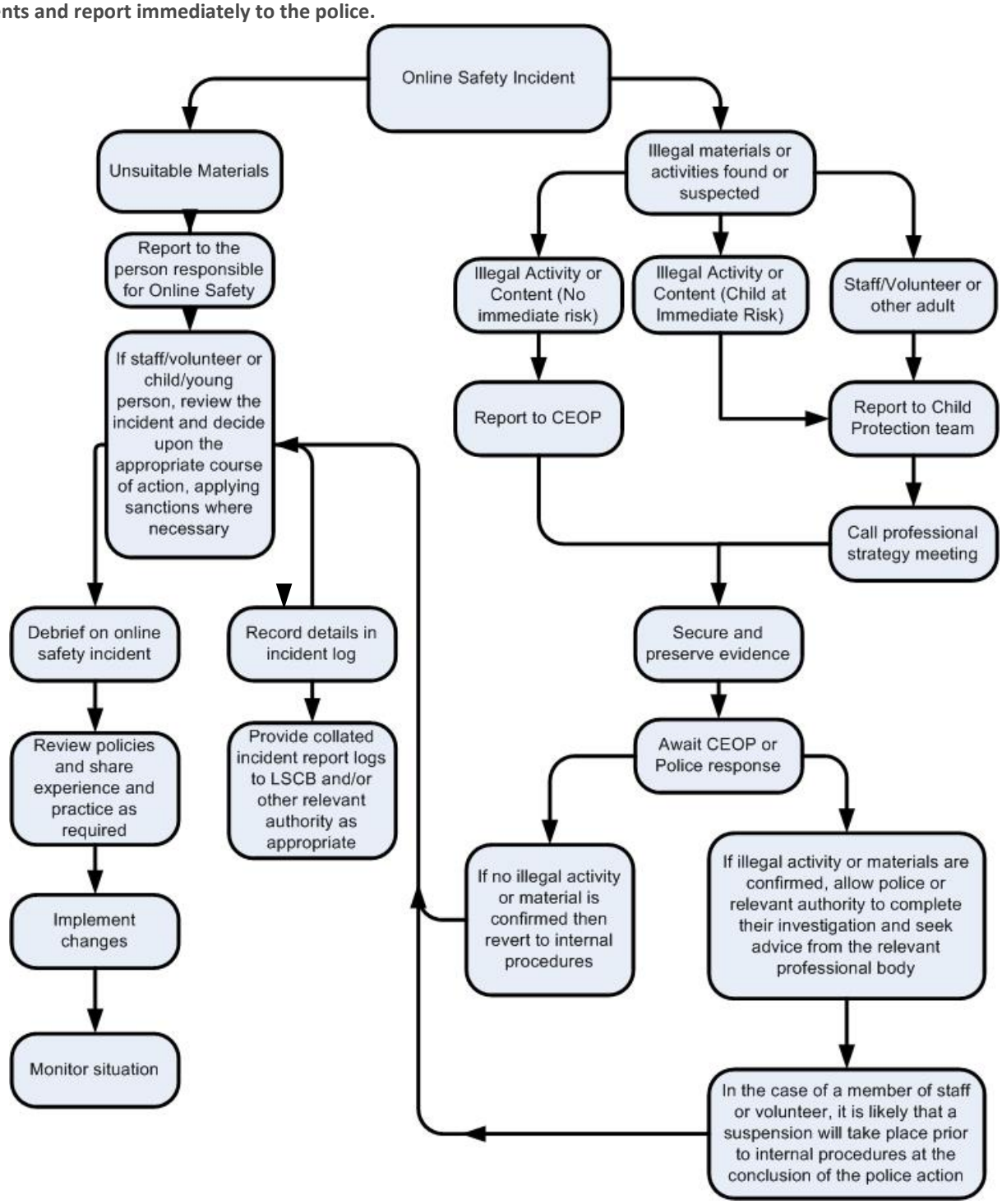
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child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



To contact the Child Exploitation Online Protection (CEOP) Agency you can use their website at;
https://www.ceop.police.uk/safety-centre/
Or their direct phone number is; 0370 496 7622 (National Crime Agency NCA).

Other Incidents

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

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

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

There is a clear distinction between staff and pupil misconduct – children are dealt with in line with this policy, whereas staff would be in line with the Employee Code of Conduct and relevant policies.

Record of School Actions & Sanctions

Students/ Pupils — Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction 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).									
Unauthorised use of non-educational sites during lessons									
Unauthorised use of mobile phone / digital camera / other mobile device									
Unauthorised use of social media / messaging apps / personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school / academy network by sharing username and passwords									
Attempting to access or accessing the school / academy network, using another student's / pupil's account									
Attempting to access or accessing the school / academy network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's / academy's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

Record of School Actions & Sanctions

Staff Actions / Sanctions

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

Acknowledgements

We would like to acknowledge the range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of the George Fentham Endowed School Online Safety Policy:

- Solihull LA/MBC
- Members of the SWGfL Online safety Group
- Child Exploitation Online Protection (CEOP)
- Childnet
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN/ Regional Broadband Grids

Appendices

Acceptable Usage Agreements