Online Safety Policy

To be read in conjunction with the
Bring Your Own Device (BYOD) Policy

BACKGROUND/RATIONALE

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students/pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school online safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Executive Head and governors to the senior leaders and classroom teachers, support staff, families, members of the community and the young people themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil/student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

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

Many of these risks reflect situations in the off-line world and it is essential that this Online safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students'/pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The Online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their families) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

DEVELOPMENT/MONITORING/REVIEW OF THIS POLICY

This policy has been developed by a working group across the Federation consisting of:

- Anne Davies - Finance/SLT
- Lynne Williams - Commissioning
- Monika Davis/Stella Taylor – Designated Safeguarding leads/SLT
- Justin Sharp/Danny Bentham – ICT Managers
- Rebecca Hughes/Nat Lowson – ICT Curriculum lead
- Amy Ley – Advocacy/Student Council
- Dave O'Loughlin – Health & Safety/Online Safety Lead

SCHEDULE FOR DEVELOPMENT/MONITORING/REVIEW

This Online safety policy was approved by the Governing Body on:	Autumn 2018
The implementation of this Online Safety policy will be monitored by the:	Online Safety Group Online Safety lead, Dave O'Loughlin – who chairs the team
Monitoring will take place at regular intervals:	Annually
The Governing Body 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 every three years, 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:	Summer 2024
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Police, LADO, LA Safeguarding Officer

The schools will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - Students
    - Families
    - Staff

SCOPE OF THE POLICY

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

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. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the federation. 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 Federation will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform families 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 with the federation.

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 Governing body receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Group
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors meeting

Executive Head and Senior Leaders:

- The Executive Head has a duty of care for ensuring the safety (including online safety) of members of the federation community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- The Executive Head/Senior Leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The Executive Head/Senior Leadership team 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 Executive Head/Senior Leadership team 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 Senior Leadership team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead:

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

Network Manager/Technical staff:

The Network Manager is responsible for ensuring:

- that the federation's technical infrastructure is secure and is not open to misuse or malicious attack
- that the federation meets the online safety technical requirements and any 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 school's 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 safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- provides training and advice for staff
- that the use of the network/internet/Learning Platform/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Executive Head/Online Safety Lead for investigation/action/sanction

- that monitoring software/systems are implemented and updated as agreed in federation policies

Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current federation Online Safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the Executive Head/Online Safety Lead for investigation/action/sanction
- all digital communications with students and families 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 understand and follow the school Online Safety Policy and acceptable use policy
- 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 and implement current policies with regard to these devices

Designated Safeguarding Lead:

Should be trained in Online Safety issues and be aware of the potential for serious child protection issues to arise from:

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

Online Safety Group:

Members of the Online Safety group will assist the Online Safety Lead with:

- the production/review/monitoring of the federation Online Safety Policy/documents.
- the production/review/monitoring of the federation filtering policy
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs
- consulting stakeholders- including families and the students about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Students – the following information will be discussed with students according to their level of understanding and abilities:

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

Families:

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

- access to parents' sections of the website and online students records
- their children's personal devices in the federation

Community Users:

Community Users who access federation systems/website as part of Hollow Lane Club activities will be expected to sign a Community User AUA before being provided with access to school systems. The Community user Manager is able to sign the agreement on behalf of staff, and will ensure staff compliance.

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 federation's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum should be provided as part of ICT/PSHE lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of lessons and 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. NB. Counter Terrorism & Securities Act 2015 requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Students should be helped to understand the need for the students Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside the federation
- 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

Education – families

Many families 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 federation will therefore seek to provide information and awareness to families through:

- Letters, newsletters, web site,
- Parents evenings
- High profile events e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. swgfl.org.uk www.saferinternet.org.uk http://www.childnet.com/parents-and-carers

Education – Wider Community

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

- Family learning courses in use of new digital technologies, digital literacy and online safety

- Online safety messages targeted towards grandparents and other relatives as well as parents

Education & Training – Staff

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

- A planned programme of formal online safety training will be made available to staff.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the federation online safety policy and Acceptable Use Agreements
- The Online Safety Lead will receive regular updates through attendance at external training events 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 meetings/training 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/group involved in technology/online safety/health and safety/safeguarding. 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 federation will be responsible for ensuring that the federation 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.

- Federation technical systems will be managed in ways that ensure that the federation meets the online safety technical requirements.
- There will be regular reviews and audits of the safety and security of federation technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to federation technical systems and devices.
- All users will be provided with a username and secure password by the ICT Manager 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 6months.

- The “master/administrator” passwords for the school ICT system, used by the ICT Manager must also be available to the Executive Head or other nominated senior leader and kept in a secure place
- The ICT 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 and it is the ICT Manager’s responsibility to ensure illegal content is filtered. 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.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Federation technical staff regularly monitor and record the activity of users on the federation technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person 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 (AUP) is in place for the provision of temporary access of ‘guests’ e.g. trainee teachers, Hollow Lane Club, visitors onto the school system.
- An agreed policy (AUP) is in place regarding the extent of personal use that users and family members are allowed on school devices that may be used out of school.
- An agreed policy (AUP) is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy (AUP) is in place regarding the use of removable media (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.

Mobile Technologies (including BYOD)

Mobile technology devices may be school owned/provided or personally owned and might include: tablet, notebook/laptop or other technology that usually has the capability of utilizing the school’s wireless network. The device then has access to the wider internet which may include the school’s learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s Online Safety education programme.

- The school 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 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 - PHOTOGRAPHIC, VIDEO

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 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 federation 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.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website/social media/local press
- Families are requested not to take videos and digital images of their children at school events for their own personal use or to publish/make publicly available on social networking sites, nor should families comment on any activities involving other students.
- Staff are allowed to take digital/video images to support educational aims, but must follow federation policies concerning the sharing, distribution and publication of those images. Those images should only be taken on federation 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 federation into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- 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.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's work can only be published with the permission of the student and families.

DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.
The federation must ensure that:

- It has a Data Protection Policy
- It has paid the appropriate fee to the Information Commissioner's Office (ICO)
- It has appointed a Data Protection Officer (DPO).
- 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 collect for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out, as required.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognizes the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions
- All schools/academies must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness/data protection training and are made aware of their responsibilities.

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 password protected.
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with federation policy once it has been transferred or its use is complete.

Communications

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

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

** FE Students are permitted use of mobile device under separate arrangement and signed agreement by families.*

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

- The official federation email service may be regarded as safe and secure and is monitored. Users should be aware that e mail communications are monitored. Staff and students should therefore use only the federation email service to communicate with others when in school.
- Users must immediately report, to the nominated person – in accordance with the federation policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or families (email, social media, chat, blogs, 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 or group email addresses may be used for students.
- Students should be taught about email 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 federation 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 behavior online is essential. Core messages should include the protection of students, the federation and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how a school protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

The federation provides the following measures to ensure reasonable steps are in place to minimize risk of harm to students, staff and the federation through:

- Ensuring that personal information is not published
- Training is provided including: 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

Federation staff should ensure that:

- No reference should be made in social media to students, families 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 federation or local authority

- Security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information

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

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behavior for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under federation disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the federation or impacts on the federation, it must be made clear that the member of staff is not communicating on behalf of the federation with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

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

The federation's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from the federation 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 federation 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 or outside the federation when using school equipment or systems. The federation 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) 0 contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behavior, including promotion of physical violence or mental harm				X	

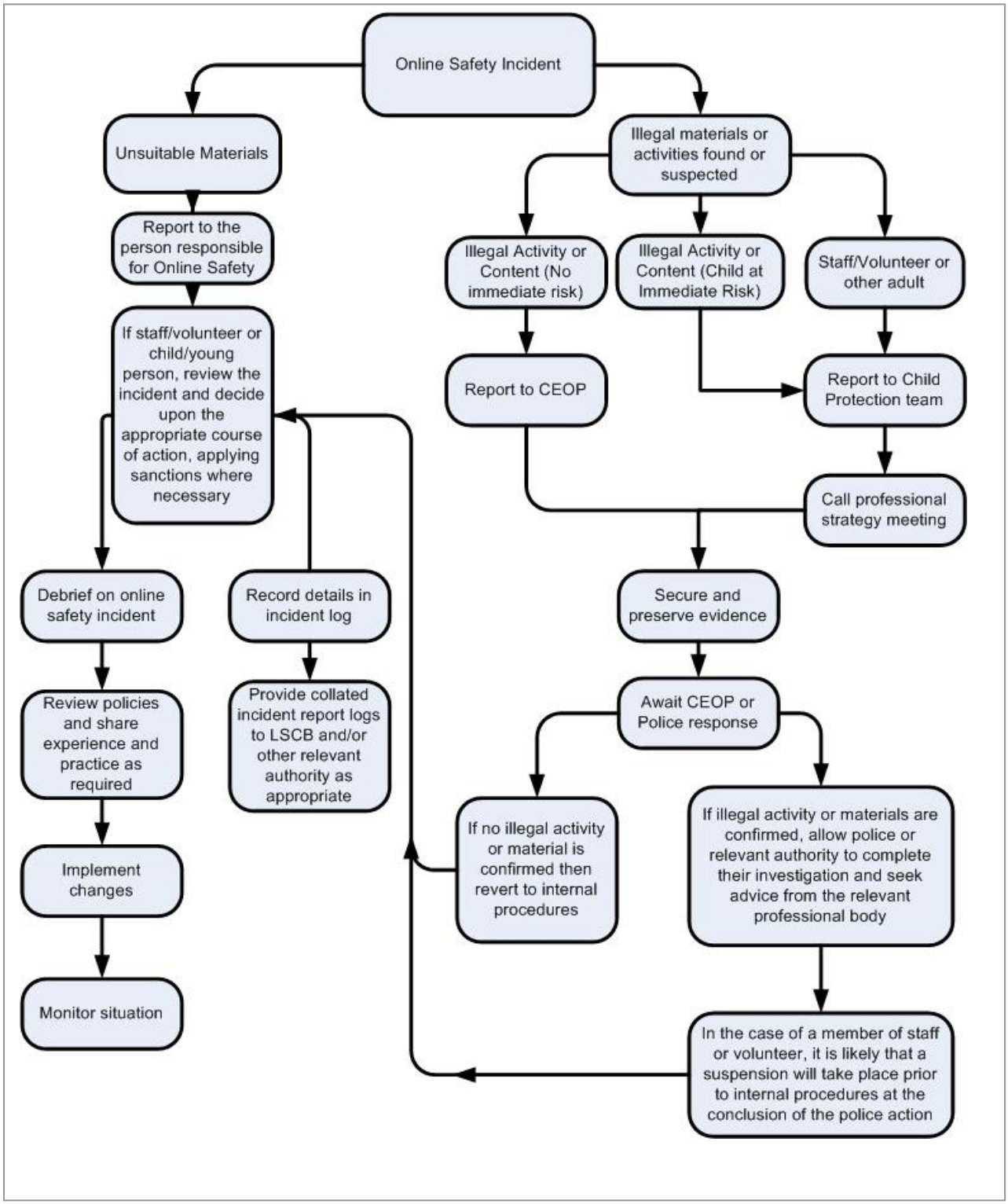
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the federation or brings the federation into disrepute				X	
Using school systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the federation					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	X			
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping/commerce			X			
File sharing						
Use of social media		X				
Use of messaging apps		X				

Use of video broadcasting e.g. You tube	X				

Responding to incidents of misuse

Illegal Incidents

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



Other Incidents
It is hoped that all members of the federation community will be responsible users of digital technologies, who understand and follow federation 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 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)
- 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/local organization as appropriate
    - 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' behavior
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - 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 federation and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form and recorded information via CPOMs should be retained by the group for evidence and reference purposes.

Federation Actions & Sanctions

It is more likely that the federation 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:

Warnings may be issued for any breaches to the following prior to action being taken:

Students/Pupils	Actions/Sanctions								
Incidents:	Refer to class teacher/tutor	Refer to Head of Department/Head of Year/other	Refer to Headteacher	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/inappropriate use of mobile phone/digital camera/other mobile device	✓								
Unauthorised/inappropriate use of social media/messaging apps/personal email	✓								
Unauthorised downloading or uploading of files	✓								
Allowing others to access federation network by sharing username and passwords	✓				✓				
Attempting to access or accessing the federation network, using another student's account	✓								
Attempting to access or accessing the federation 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 federation into disrepute or breach the integrity of the ethos of the school	✓								
Using proxy sites or other means to subvert the federation'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	✓								

Warnings may be issued for any breaches to the following prior to action being taken:

Staff Actions/Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	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 federation network by sharing username and passwords or attempting to access or accessing the federation 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		✓	✓					
Actions which could compromise the staff member's professional standing		✓						✓
Actions which could bring the federation into disrepute or breach the integrity of the ethos of the federation		✓						✓
Using proxy sites or other means to subvert the school'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		✓			✓			

STUDENT ACCEPTABLE USE AGREEMENT FORM (THERE IS NO EXPECTATION OF A SIGNATURE UNLESS DEEMED USEFUL FOR A STUDENT)

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

I have read and understand the above and agree to follow these guidelines when:

- I use the Federation systems and devices in school
- I use my own devices in school (when allowed), in accordance with the BYOD Policy.
- I use my own equipment out of the school in a way that is related to me being a member of this Federation e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil: .....

Group / Class: .....

Signed: .....

Date: .....

STUDENT ACCEPTABLE USE POLICY AGREEMENT

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): .....

Signed (parent): .....

STAFF INFORMATION SYSTEMS CODE OF CONDUCT

I understand that l must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

- I will comply with the Federation's Data Protection Policy.
- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role at all times.
- I understand that school information systems may not be used for private purposes, without specific permission from the Executive Head.
- I understand that the school may monitor my use of information systems and the Internet to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I understand that to enhance security my password will need to be changed on a regular basis.
- I will not install any software or hardware without permission from the ICT Technician/Executive Head.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will ensure that any data taken off school premises is stored on an encrypted school USB memory stick, password protected laptop or Learn to Live Federation 0365 tenancy.
- I acknowledge that USB memory sticks are for the secure transportation of work to and from school and that USB memory sticks are not to be used to store information long term.
- I will respect copyright and intellectual property rights, and will liaise with the ICT technician regarding any use of music in lessons, clubs, performances or video recordings.
- I will report any incidents of concern regarding children's safety to the Designated Senior Person for Child Protection/Safeguarding.

- I will report any incidents of concern regarding use of the internet, filtering and Online Safety to the Network Manager or Online Safety coordinator
- I understand that I am responsible for the appropriate use of any school IT equipment issued to me and for the actions of any others that I allow to use it.
- I understand that I must report any faults with IT equipment issued to me to the Network Manager when they occur and that these items may be recalled on a regular basis for monitoring and updating.
- I will ensure that any electronic communications with pupils or parents/carers are compatible with my professional role.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will comply with the Devon County Council guidelines that electronically held images should be held in a password protected directory with restricted access and ensure that only authorised access can take place
- I will comply with the Learn to Live Social Media Policy.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or storing unauthorised or unlawful text, imagery or sound.

Staff Agreement Form

I have read, understood and agree with the Information Systems Code of Conduct

Signed ……Print ……Date …….

Accepted for school: ……. Print ……..

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of the Federation digital technologies will be responsible users and stay safe while using these systems and devices
- that the Federation 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
If this document is signed by a Manager on behalf of the Community Users, it is their responsibility to ensure all staff adhere to the following:

I understand that l must use the Federation 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 l bring into the Federation.

- I understand that my use of Federation systems and devices and digital communications will be monitored
- I will not use a personal device that l 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, l 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 l take and/or publish images of others l 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 l have obtained whilst in the school on any personal website, social networking site or through any other means, unless l 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 l try to alter computer settings, unless l have permission to do so.
- I will not disable or cause any damage to Federation 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 l have permission to use the original work of others in my own work
- Where work is protected by copyright, l will not download or distribute copies (including music and videos)
- I understand that if l fail to comply with this Acceptable Use Agreement, the Federation has the right to remove my access to the Federation systems/devices.

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

SCHOOL FILTERING POLICY

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. It is therefore 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.
As a part of the South West Grid for Learning (SWGfL) schools and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

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 SWGfL/school filtering service must:

- be logged in change control logs
- be reported to the E-Safety Co-ordinator each term in the form of an audit of the change control logs

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

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

Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the e-safety education programme. Staff users will be made aware of the filtering systems through:

- signing the AUP
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions/newsletter etc.

Changes to the Filtering System

Users may request changes to the filtering system by contacting the Network Manager. Changes will be allowed only if there are strong educational reasons for doing so and The Network Manager will refer the matter to the E-Safety Co-ordinator for approval.

All changes should be reported via the Change Log which will be reviewed by the E Safety Co-ordinator or termly.

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 Network Manager who will decide whether to make school level changes. If it is felt that the site

should be filtered (or unfiltered) at SWGfL level, the Network Manager should email filtering@swgfl.org.uk with the URL.

Monitoring

ICT Managers will monitor the filtering systems using appropriate software.

Audit/Reporting

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

- the E Safety Co-ordinator
- Online Safety Lead
- E-Safety Group
- E-Safety Governors
- SWGfL/Local Authority 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 PASSWORD SECURITY POLICY

Introduction

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as 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

A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems.

Responsibilities

The management of the password security policy will be the responsibility of the Network Manager. All users 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.

Training/Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. Members of staff will be made aware of the school's password policy:

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

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

Policy Statements

All users will have clearly defined access rights to school ICT 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 E-Safety Committee.

All 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. Users will be required to change their password periodically.

The "master/administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Executive Head or other nominated senior leader and kept in the school safe.

Audit/Monitoring/Reporting/Review

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

- User ID's and requests for password changes
- User log-on's
- Security incidents related to this policy

In the event of a serious security incident:

- the police may request and will be allowed access to passwords used for encryption.
- Local Authority Auditors also have the right of access to passwords for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner. These records will be reviewed by E-Safety Officer at regular intervals. This policy will be regularly reviewed annually in response to changes in guidance and evidence gained from the logs.