West Exmoor Federation

E-Safety Policy

March 2019

West Exmoor Federation –E-Safety Policy

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. The Governor responsible for Safeguarding is also responsible for E-Safety. The role of the E-Safety Governor will include:

- regular meetings with the Safeguarding Officer;
- regular monitoring of e-safety incident logs;
- reporting to relevant Full Governing Body Meetings.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the federation community, though the day to day responsibility for e-safety will be delegated to the Safeguarding officer.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher / Senior Leaders are responsible for ensuring that the Safeguarding Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

Safeguarding Officer:

- Leads e-safety at Governing Body and staff level;
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy;
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Provides or facilitates training and advice for staff;
- Liaises with the Local Authority / SWGfL;
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- Attends relevant Governors committee meetings;
- Reports regularly to Senior Leadership Team;

Network Manager / Technical staff

ScoMis is responsible for overseeing:

- That the federations' technical infrastructure is secure and is not open to misuse or malicious attack;

- That the federation meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply;
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- The filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant;
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction;
- That monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current *school* e-safety policy and practices;
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP;)
- They report any suspected misuse or problem to the *Headteacher* / *E-Safety Coordinator* / *Safeguarding Officer* for investigation / action / sanction;
- All digital communications with pupils / parents / carers should be on a professional level.
- E-safety issues are embedded in all aspects of the curriculum and other activities;
- Pupils understand and follow the e-safety and acceptable use policies;
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other federation activities (where allowed) and implement current policies with regard to these devices;
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Safeguarding Officer

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data;
- Access to illegal / inappropriate materials;
- Inappropriate on-line contact with adults / strangers;
- Potential or actual incidents of grooming;
- Cyber-bullying.

Pupils

Are taught about:

- Using the federation's digital technology systems in accordance with the Pupil Acceptable Use Policy;
- The need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- 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.
- The importance of adopting good e-safety practice when using digital technologies out of school and realise that the federation's E-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 federation will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the federation in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at federation events;

- access to parents' sections of the website;
- their children's personal devices in the school (where this is allowed).

Policy Statements

Education – students / pupils

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

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

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited;
- Key e-safety messages should be reinforced as part of a planned programme of collective worship;
- Pupils 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;
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school;
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices;
- In lessons where internet use is pre-planned, it is best practice that 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;
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – parents / carers

Many parents and carers have only a limited understanding of e-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 parents and carers through:

- Letters, newsletters, web site, VLE;
- Parents / Carers evenings / sessions;
- High profile events / campaigns eg Safer Internet Day;
- Reference to the relevant web sites / publications.

Education & Training – Staff / Volunteers

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

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

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / e-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 (eg SWGfL);
- 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's infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

- School technical systems will be managed in ways that ensure that the federations meets recommended technical requirements;
- There will be regular reviews and audits of the safety and security of school technical systems;
- Servers, wireless systems and cabling must be securely located and physical access restricted;
- All users will have clearly defined access rights to school technical systems and devices;
- All users will be provided with a username;
- The administrator passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place (eg school safe);
- The Administrator 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 by default;
- The federation has provided enhanced / differentiated user-level filtering. Teaching staff are able to bypass the filtering to access teaching resources using sites normally restricted – eg youtube;
- 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.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils 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 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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images;

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs;
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Data Protection

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

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

The federation must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for;
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay;
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section in the appendix);
- It has a Data Protection Policy;
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA);
- 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;
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.

Staff must ensure that they:

- 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;
- 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

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 email communications are monitored;
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication;
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content;

- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies;
- Personal information should not be posted on the federation website and only official email addresses should be used to identify members of staff.

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

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

Unsuitable / inappropriate 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 school or outside school 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) - 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	

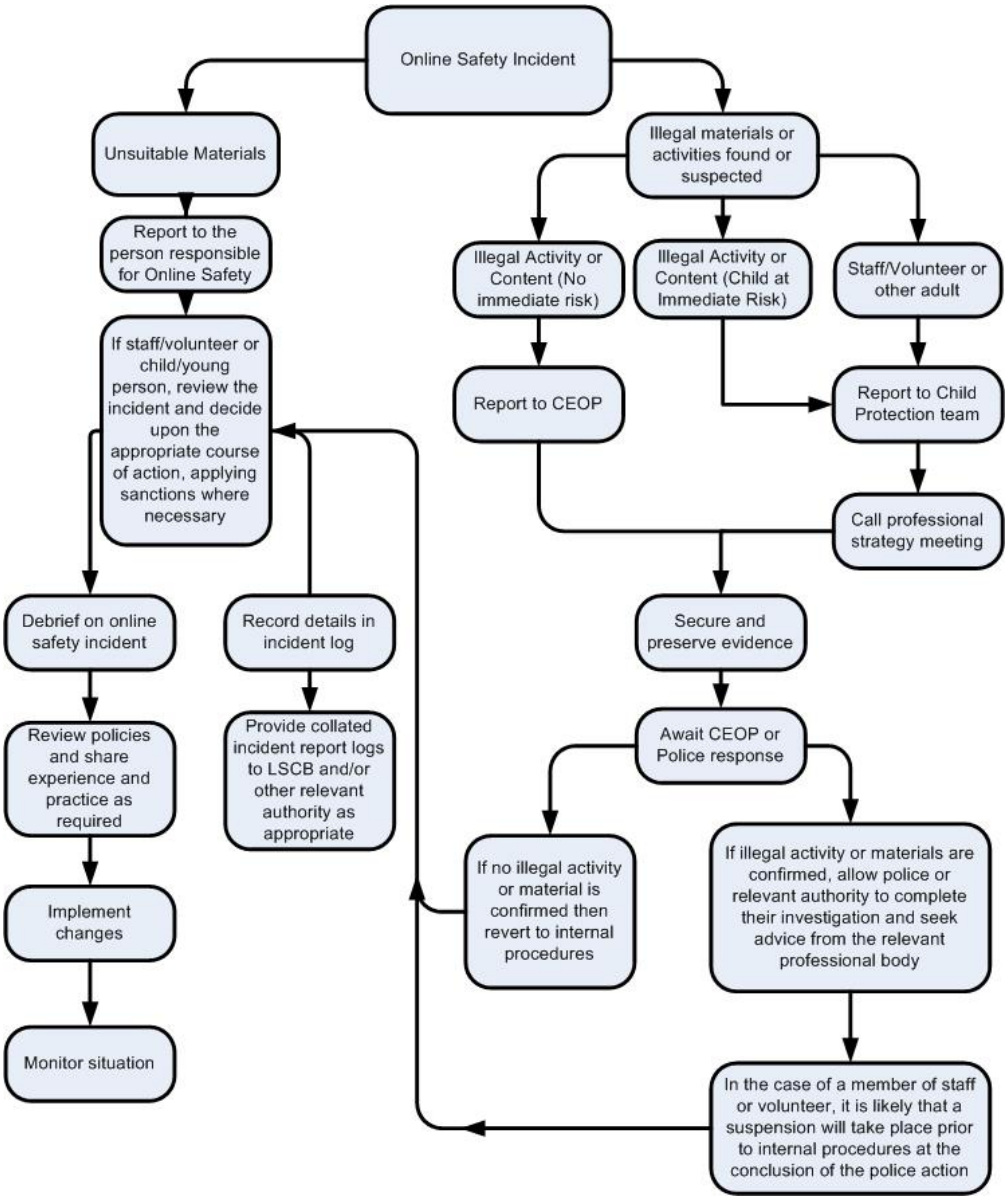
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy			X		
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)				X	
On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting eg Youtube, vimeo.			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.



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

- Involvement by Local Authority or national / local organisation (as relevant);
- Police involvement and/or action.

- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the 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 federation 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 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 federation 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:

Pupils — Actions / Sanctions

Incidents:	Refer to class teacher	Refer to SDO and safety officer.	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 eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X	X			X		X	
Unauthorised use of social media / messaging apps / personal email	X		X			X		X	
Unauthorised downloading or uploading of files	X				X		X		
Allowing others to access school network by sharing username and passwords (Unauthorised)	X						X	X	
Attempting to access or accessing the school network, using another pupil's account. (unauthorised)	X	X	X			X	X	X	
Attempting to access or accessing the school / academy network, using the account of a member of staff	X	X	X		X	X	X	X	Red card
Corrupting or destroying the data of other users	X	X	X		X	X	X	X	Red card
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X	X	X	Red card

Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X	X	X	
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	?	X	X	X	X	Red card
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X					X	

Staff Actions / Sanctions

Incidents:	Refer to SDO and safety officer	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).	X	X	X	X				
Inappropriate personal use of the internet / social media / personal email (Depending on severity.)	X	X	X	X	X			
Unauthorised downloading or uploading of files (Depending on severity.)	X	X	X	X	X			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account (Depending on severity.)	X	X	X	X	X			
Careless use of personal data eg holding or transferring data in an insecure manner	X	X			X			
Deliberate actions to breach data protection or network security rules	X	X		X	X			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X		X	X			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature (Depending on severity)	X	X	X	X	X			
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X	X	X			
Actions which could compromise the staff member's professional standing	X	X	X			X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X				X		

Unauthorised use of proxy sites or other means to subvert the school's filtering system	X	X				X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X			
Breaching copyright or licensing regulations	X	X				X		
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X			

Pupil Acceptable Use Agreement - KS2

Federation Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use;
- That fchool systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The federation will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use federation ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the federation will monitor my use of the systems, devices and digital communications;
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it;
- I will be aware of "stranger danger", when I am communicating on-line;
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc);
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me;
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that the federation systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

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

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

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

- I will not use my own personal devices – eg. Mobile phone, digital camera or other hand held devices, in school;
- I will immediately report any damage or faults involving equipment or software, however this may have happened;
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings;
- I will only use social media sites with permission and at the times that are allowed. Eg learning blogs.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work;
- Where work is protected by copyright, I will not try to download copies (including music and videos);

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the federation also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the federation community (examples would be cyber-bullying, use of images or personal information);
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the federation network / internet, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

Pupil Acceptable Use Agreement Form

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

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

- I use the federation systems and devices (both in and out of school);
- I use my own devices in the school (when allowed) eg mobile phones, gaming devices USB devices, cameras etc;
- I use my own equipment out of the school in a way that is related to me being a member of the federation, eg communicating with other members of the school, website etc.

Name	
Class	
Signed	
Date	

Pupil Acceptable Use Agreement Form – Foundation Stage/Key Stage 1

<u>This is how we stay safe when we use computers:</u>

I will ask a teacher or suitable adult if I want to use the computers;

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.

Signed (child):……

Parent/Carer Acceptable Use Agreement Form

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- That federation systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- That parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The federation will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents and carers will be aware of the federaiton expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the federation in this important aspect of the federation's work.

Permission Form

Parent / Carers Name | Pupil(s) Name

As the parent/carer of the above pupil(s), I give permission for my son/daughter to have access to the internet and to ICT systems within the federation.

(KS2)
I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

(KS1)
I understand that the federation has discussed the Acceptable Use Agreement with my son/daughter and that they have received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the federation will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the federaiton cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the federation will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the federation if I have concerns over my child's e-safety.

Signed | Date

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- That federation ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- That staff are protected from potential risk in their use of ICT in their everyday work.

The federation will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the federation will monitor my use of the ICT systems, email and other digital communications;
- I understand that the rules set out in this agreement also apply to use of federation ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school;
- I understand that the federation ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the federation;
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it;
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission;
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions;
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the federation's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured;
- I will not use chat and social networking sites in school;
- I will only communicate with pupils and parents/carers using official federaiton systems. Any such communication will be professional in tone and manner;
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using federation equipment. I will also follow any additional rules set by the federation about such use.
- I will not use personal email addresses on the school ICT systems;
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes);
- I will ensure that my data is regularly backed up, in accordance with relevant federaiton policies;
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials;
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work;
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in federation policies;
- I will not disable or cause any damage to federation equipment, or the equipment belonging to others;
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Federation's Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage;
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by federation policy to disclose such information to an appropriate authority;
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for federaiton sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work;
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

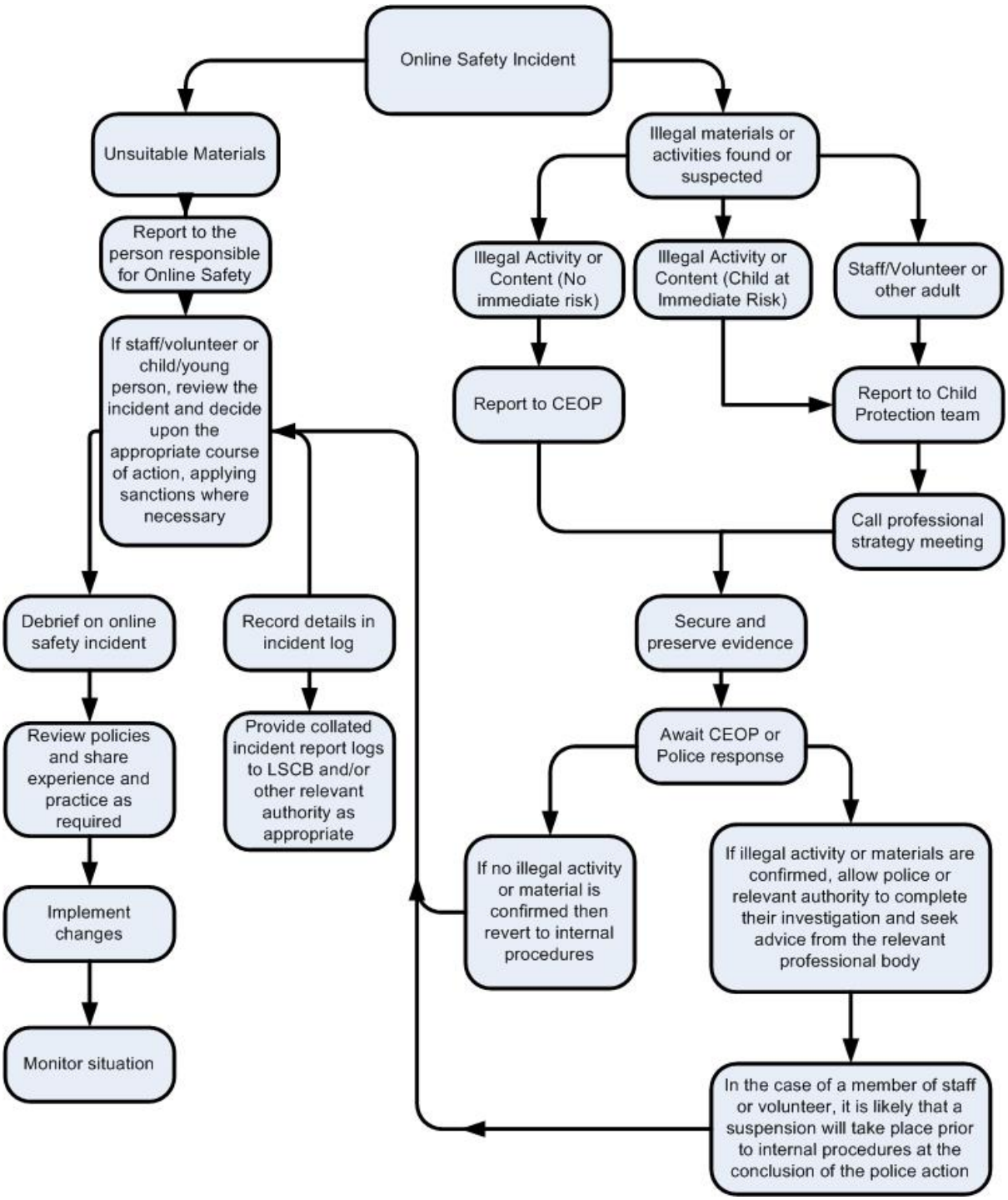
I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of federation ICT equipment in school, but also applies to my use of federation ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the federation.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff / Volunteer Name	
Signed	
Date	

Responding to incidents of misuse – flow chart



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

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

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

Web site(s) address / device	**Reason for concern**

Conclusion and Action proposed or taken

Template Reporting Log

Reporting Log Group										
Date	Time	Incident	Action taken		Incident Reported by	Signature				
			What?	By whom?						

Training Needs Audit

Training Needs Audit Log

Group ..... Date .....

Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date

What policies and procedures should be put in place for individual users of cloud-based services?
The federation is ultimately responsible for the contract with the provider of the system, so check the terms and conditions carefully; below is a list of questions that you may want to consider when selecting a cloud services provider; indeed you may want to contact any potential provider and ask them for responses to each of the following:

- How often is the data backed up?
- Does the service provider have a clear process for you to recover data?
- Who owns the data that you store on the platform?
- How does the service provider protect your privacy?
- Who has access to the data?
- Is personal information shared with anyone else? Look out for opt in/opt out features
- Does the service provider share contact details with third party advertisers? Or serve users with ads?
- What steps does the service provider take to ensure that your information is secure?
- Is encryption used? Is https used as default or is there an option to use this? Two step verification?
- How will your data be protected? Look out for features that will keep your information safe and secure including Anti-spam, Anti-Virus and Anti-malware…
- How reliable is the system? Look out for availability guarantees.
- What level of support is offered as part of the service? Look out for online and telephone support, service guarantees

SWGfL provides a useful summary of these issues in a document that has been written with the support of Google and Microsoft:

http://www.swgfl.org.uk/News/Content/News-Articles/Cloud-based-products-and-services

The document focuses on Google Apps for Education and Microsoft 365, but poses important considerations if a school is considering services from another provider.

Parental permission for use of cloud hosted services
Schools that use cloud hosting services (eg.Google Aps for Education) may be required to seek parental permission to set up an account for pupils/students.

Google Apps for Education services - http://www.google.com/apps/intl/en/terms/education_terms.html requires a school to obtain 'verifiable parental consent'. Normally, schools will incorporate this into their standard acceptable use consent forms sent to parents each year (see suggested wording on "Parent/Carer Acceptable Use Agreement Template").

A template form has been added to the Parents & Carers Acceptable User Template elsewhere in these Template Policies.

Links to other organisations or documents

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

UK Safer Internet Centre

Safer Internet Centre -

South West Grid for Learning

Childnet

Professionals Online Safety Helpline

Internet Watch Foundation

CEOP

http://ceop.police.uk/ ThinkUKnow

Others:

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

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

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

Cyberbullying

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government Better relationships, better learning, better behaviour

DCSF - Cyberbullying guidance

DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies

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

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

Social Networking

Digizen – Social Networking

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people

Connectsafely Parents Guide to Facebook

Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

Glow - http://www.educationscotland.gov.uk/usingglowandict/

Alberta, Canada - digital citizenship policy development guide.pdf

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Somerset - e-Sense materials for schools

Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People

Kent - Safer Practice with Technology

Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs

Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs

UK Safer Internet Centre Professionals Online Safety Helpline

Working with parents and carers

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

SWGfL BOOST Presentations - parents presentation

Connect Safely - a Parents Guide to Facebook

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

DirectGov - Internet Safety for parents

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

The Cybersmile Foundation (cyberbullying) - advice for parents

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Futurelab - "Digital participation - its not chalk and talk any more!"