NAWTON AND ROSEDALE ABBEY COMMUNITY PRIMARY SCHOOL FEDERATION

ONLINE SAFETY POLICY

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school sites and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the schools, but are linked to membership of the schools.

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

Policy Statements

Education – 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 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 is provided as part of Computing and PHSE
- Key online safety messages are reinforced as part of a planned programme of assemblies
- 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 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.
- Pupils will be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff will 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.
- When pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Parents and carers may have 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 therefore seeks to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, Learning Platform
- Annual parent / carers online safety sessions
- High profile events / campaigns e.g. Safer Internet Day

Education – The Wider Community

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

- Providing 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.
- The schools websites will provide online safety information for the wider community

Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out annually.
- 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.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator 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 staff meetings and at PD Days when appropriate
- The Online Safety Coordinator provide advice, guidance and training to individuals as required.

Training – Governors

Governors should take part in online safety training and awareness sessions, with particular importance for the Online Safety Governor. 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 information sessions for staff or parents (this may include attendance at assemblies / lessons).

Roles and Responsibilities

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

The Governing Body:

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 receiving regular information about online safety incidents and monitoring reports.

Sheryl Woodward is the delegated member of the Governing Body for Online Safety.

The role of the Online Safety Governor / Director will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings

- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to the full Governing Body

The Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and the day to day responsibility for online safety. The Headteacher and Senior Teachers are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff - see flow chart on dealing with online safety incidents.
- The Headteacher is responsible for ensuring that all staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher ensures 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.

Online Safety Coordinator:

The Online Safety Coordinator is Miss Nichola Oxtoby - Headteacher

- 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 / relevant body
- 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 the Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs

Network Manager / Technical staff:

The Nawton and Rosedale Abbey Community Schools Federation has a managed ICT service provided by NYCC.

The Network Manager / Technical Staff is responsible for ensuring:

- that the schools technical infrastructure is secure and is not open to misuse or malicious attack

- that the schools meet required online safety technical requirements and any Local Authority Online 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 (see appendix "Technical Security Policy Template" for good practice)
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network, internet and email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher
- that monitoring software and 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 online safety matters and of the current Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher for investigation, action or sanction
- all digital communications with students, pupils, parents and carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy 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 school 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

Designated Safeguarding Lead

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

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers

- potential or actual incidents of grooming
- cyber-bullying

It is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the Federation community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.
The group will also be responsible for regular reporting to the Governing Body.

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

- the production, review and monitoring of the school Online Safety Policy and documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network, internet and incident logs
- consulting stakeholders – including parents / carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

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

Parents / Carers

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

campaigns and literature. Parents and carers will be encouraged to support the Federation in promoting good online safety practice and to follow guidelines on the appropriate use of:
digital and video images taken at school events
their children's personal devices in the school

Technical – infrastructure, equipment, filtering and monitoring

It is the responsibility of the Federation to ensure that the managed service provider (NYCC) carries out all the online safety measures that would otherwise be the responsibility of the Federation. It is essential that the managed service provider is fully aware of the Federation's Online Safety Policy and Acceptable Use Agreements
The Federation will be responsible for ensuring that the school network are as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School / Academy technical systems will be managed in ways that ensure that the Federation meets recommended technical requirements
- There are regular reviews and audits of the safety and security of the 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, staff and all KS1 and KS2 children, will be provided with a username and secure password by The School Administrator who will keep an up to date record of users and their usernames in locked storage. Users are responsible for the security of their username and password and will be required to change their password every year
- The "master administrator" passwords for the Federation ICT system, used by the Network Manager must also be available to the Headteacher and kept in the school safe.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering ensures that children are safe from terrorist and extremist material when accessing the internet
- The Federation has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different groups of users – staff / pupils.
- School / academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use

Agreement. An appropriate system is in place for users to report any actual or potential technical incident or security breach to the relevant person, as agreed).

- Appropriate security measures are in to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place (to be described) that allows staff to download executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks) 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

All users should understand that the primary purpose of the use mobile devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety curriculum.
The school Acceptable Use Agreements for staff, pupils and parents/carers gives consideration to the use of mobile technologies.

The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	√	√	√	√	√	√
Full network access	√	√	√	x	x	x
Internet only	n/a	n/a	n/a	n/a	n/a	n/a
No network access	n/a	n/a	n/a	√	√	√

Personal devices:

- Staff and visitor personal devices must remain turned off during teaching time, unless specific permission has been granted by the Headteacher.
- Staff and visitors mobile devices must not be visible to pupils, unless specific permission has been granted by the Headteacher.
- Staff may only use their personal devices in non-teaching areas i.e. offices and staffroom during the school day.
- Staff may use personal devices before 8:30am and after 3:30pm with the exception of staff working in the Schools Out Club and After School Activities and Clubs.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing 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 school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate 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 e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, social media or in the local press - see Parents / Carers Acceptable Use Agreement.

Use of digital and video images – Parents/ Carers

- 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 or made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Use of digital and video images – Staff/ Volunteers

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on

school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the student / pupil and parents or carers.

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
- 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
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

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

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 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 federation currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

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

In addition:

- The 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 Headteacher in accordance with the school 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 parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may **only** take place on official (monitored) federation systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses are used in KS1, while pupils in KS2 and above will be provided with individual school email addresses for educational use.
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate

communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information will not be posted on the school websites and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities can 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 Federation or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school / academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school 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

School / academy staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or Federation 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 minimise risk of loss of personal information

When official school / academy social media accounts are established there should be:

- A process for approval by the Headteacher
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including:

1. Systems for reporting and dealing with abuse and misuse
2. Understanding of how incidents may be dealt with under school / academy 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
The Federation permits reasonable and appropriate access to private social media sites.

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 school
The school should effectively respond to social media comments made by others according to a defined policy or process
The Federations use of social media for professional purposes will be checked regularly by the Headteacher and Online Safety Group to ensure compliance with the school policies.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from 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 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	
	Promotion of extremism or terrorism				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	

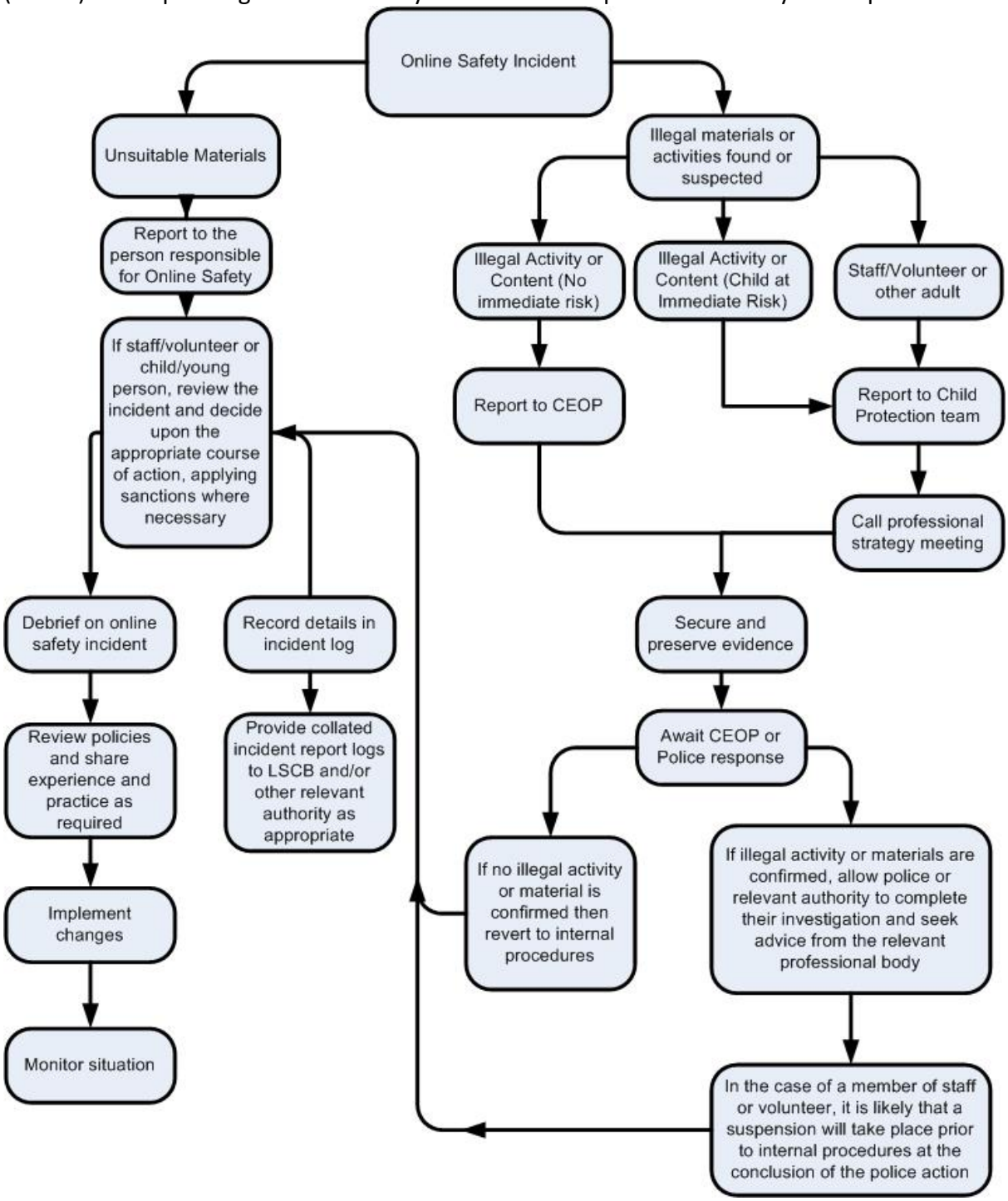
On-line gaming (educational)	x				
On-line gaming (non-educational)				x	
On-line gambling				x	
On-line shopping / commerce		x			
File sharing		x			
Use of social media		x			
Use of messaging apps		x			
Use of video broadcasting e.g. Youtube		x			

Responding to incidents of misuse

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

Illegal Incidents

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



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 – 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:

1. Internal response or discipline procedures
2. Involvement by Local Authority or national / local organisation (as relevant).
3. 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:

    1. incidents of 'grooming' behaviour
    2. the sending of obscene materials to a child
    3. adult material which potentially breaches the Obscene Publications Act
    4. criminally racist material
    5. promotion of terrorism or extremism
    6. 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 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 our disciplinary procedures.