Hanham Primary Federation

Online Safety Policy

Development / Monitoring / Review of this Policy

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

- Headteacher / Principal / Senior Leaders. *Gabby Howells, Matthew Norcott, Helen Lees*
- Online Safety Officer / Coordinator *Jo Edwards and Daniel Wake*
- Staff – including Teachers, Support Staff, Technical staff: Integra
- Governors
- Parents and Carers: Parent Forum
- Community users: Hanham Primary Federation After School Club

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

Schedule for Development / Monitoring / Review

The implementation of this Online Safety policy will be monitored by the:	*FGB*
Monitoring will take place at regular intervals:	*Annually*

The Governing Body receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:???	*Annually*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, LADO, Police*

The Federation will monitor the impact of the policy using:

- Logs of reported incidents on CPOMS
- Monitoring logs of internet activity (including sites visited) / filtering: through Integra
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of the *Federation* (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 students / pupils when they are off the *Federation* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the *Federation,* but is linked to membership of the Federation. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy).

Roles and Responsibilities

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

Governing Body

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This falls under the remit of the Safeguarding governors and relies on them receiving regular information about online safety incidents and monitoring reports. Governor duties include:

- annual meetings with the Computing Leads/E-Safety Co-ordinators

- regular monitoring of online safety incident logs on CPOMS
- regular monitoring of filtering / change control logs (feedback from Integra)
- reporting to relevant Governors / Board / Committee / meeting

Headteacher and Senior Leaders:

- The Executive Headteacher has a duty of care for ensuring the safety (including online safety) of members of the Federation community, though the day to day responsibility for online safety will be delegated to the Computing Leads/E-Safety Co-ordinators.
- The Executive 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 online safety allegation being made against a member of staff
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in the Federation who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Computing Leads/E-Safety Coordinators

Computing Leads/E-Safety Co-ordinators:

- take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the Federation online safety policies
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provide training and advice for staff
- liaise with Integra technical staff
- receive reports of online safety incidents and creates a log of incidents to inform future online safety developments, meets annually with Safeguarding Governors to discuss current issues, review incident logs and filtering / change control logs
- report to Federation Leadership Team

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current *Federation* Online Safety Policy and practices https://www.jigsawpshe.com/jigsaw-and-the-latest-ofsted-guidance-2016-on-safeguarding/
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP) see Federation Partnership book
- they have read and signed the federation Social Media Policy
- they report any suspected misuse or problem to the *Headteacher* for investigation / action / sanction

- all digital communications with parents / carers should be on a professional level *and only carried out using official Federation systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety Policy and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other Federation activities (where allowed) and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned, students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

Designated Safeguarding Leads

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

Students / Pupils:

- are responsible for using the *Federation* digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement
- 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. (People shouldn't be photographed without permission, consider the use of the image)
- should understand the importance of adopting good online safety practice when using digital technologies out of Federation and realise that the *Federation's* Online Safety Policy covers their actions out of Federation, if related to their membership of the Federation

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 and information about national / local online safety campaigns / 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 Federation events
- access to parents' sections of the website and on-line student / pupil records
- their children's personal devices in the Federation

Policy Statements

Education – Students / Pupils

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

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

- A planned online safety curriculum should be provided as part of Computing / JIGSAW / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and circletime activities
- 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 decisionmaking
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students / 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 students / 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 online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

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

Education & 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:

- The Computing Lead/E-Safety Co-ordinator is responsible for sharing important updates with staff. For example, information about a new form of social media that is becoming popular with pupils.
- 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
- This Online Safety Policy and its updates will be presented to and discussed by staff as part of the annual safeguarding and child protection training.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who have a specific responsibility for safeguarding.

Technical – infrastructure / equipment, filtering and monitoring

The technical maintainance of the Federation's systems and networks is managed by Integra IT services. They are responsible for ensuring that the following takes place:

- There will be regular reviews and audits of the safety and security of Federation technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to Federation technical systems and devices
- The "master / administrator" passwords for the Federation used by the Network Manager (or other person) must also be available to the *Headteacher* and kept in a secure place (eg school safe)

- The School Business Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- **Internet filtering will ensure that children are safe from terrorist and extremist material when accessing the internet.**
- *Integra ICT technical staff regularly monitor and record the activity of users on the Federation technical systems and users are made aware of this in the Acceptable Use Agreement*
- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed)*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the Federation systems and data. These are tested regularly. The Federation 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 Federation 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 Federation devices that may be used out of Federation*
- *An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on Federation devices*
- *An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on Federation devices.* ***Personal data cannot be sent over the internet or taken off the Federation site unless safely encrypted or otherwise secured***

Mobile Technologies

 The Federation Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies The Federation allows:

	Federation Devices			Personal Devices		
	Federation owned for single user	**Federation owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed to be used in Federation	*Yes*	*Yes*	*Yes*	*No*	*Yes**	*No*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only	*NA*	*NA*	*NA*	*No*	*No*	*No*
No network access	*NA*	*NA*	*NA*	*Yes*	*Yes*	*yes*

***Outside class time**

Only Year 6 children may bring mobile devices to school as we recognise they may be needed when children are walking home independently. These are to be switched off and passed to teachers to be locked away in a safe place in the classroom during registration time at the start of the school day. Children will receive these when dismissed by their teacher. Children attending a club must hand these to club leaders and will receive them upon leaving the club. Children may only switch them on as they leave the site via the main gates. Children using a device outside of these specified times will be challenged by staff and staff have the right under the Education Act (2011) to confiscate a device or deny it's return should we feel there is a risk to a child's safety or wellbeing. The school is not liable and does not accept responsibility for loss, theft of damage of the device. Storing them has the sole function of safeguarding children and not as a way of protecting property.

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the Federation.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils' instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The Federation will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate students / 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 students / pupils are published on the Federation website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at Federation 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 *students / pupils* in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow Federation policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Federation equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Federation 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.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the GDPR Regulations 2018 which state 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"
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- 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

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				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the Federation		Y		N				
Mobile phones may be brought in but must be in the office during the Federation day					Y			
Use of mobile phones in lessons		N		N				
Use of mobile phones in social time		Y		N				
Taking photos on personal mobile phones / cameras		N		N				
Taking photos on Federation devices	Y				Y			
Use of other mobile devices e.g. tablets, gaming devices		N		N				
Use of personal email addresses in Federation , or on Federation network			N					N
Use of Federation email for personal emails		N						
Use of messaging apps		N						
Use of social media (Federation Only)		Y*						
Use of blogs		Y						

*During non-teaching time (e.g. lunchbreak)

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.** *Staff and pupils should therefore use only the Federation email service to communicate with others when in Federation, or on Federation systems (e.g. by remote access)*
- **Users must immediately report, to the nominated person – in accordance with the Federation policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication**
- **Any digital communication between staff / pupils or parents / carers 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.*

- *Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the 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 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 *Federation* 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 Federation through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions Risk assessment, including legal risk Federation staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or Federation 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

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

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

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the Federation or impacts on the Federation, it must be made clear that the member of staff is not communicating on behalf of the Federation with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the Federation are outside the scope of this policy

- Where excessive personal use of social media in Federation is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

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

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from 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 Federation 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 Federation context and that users, as defined below, should not engage in these activities in / or outside the Federation when using Federation 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,	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 Federation or brings the Federation into disrepute				X	
Using Federation systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Federation					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (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				

*Class Dojo

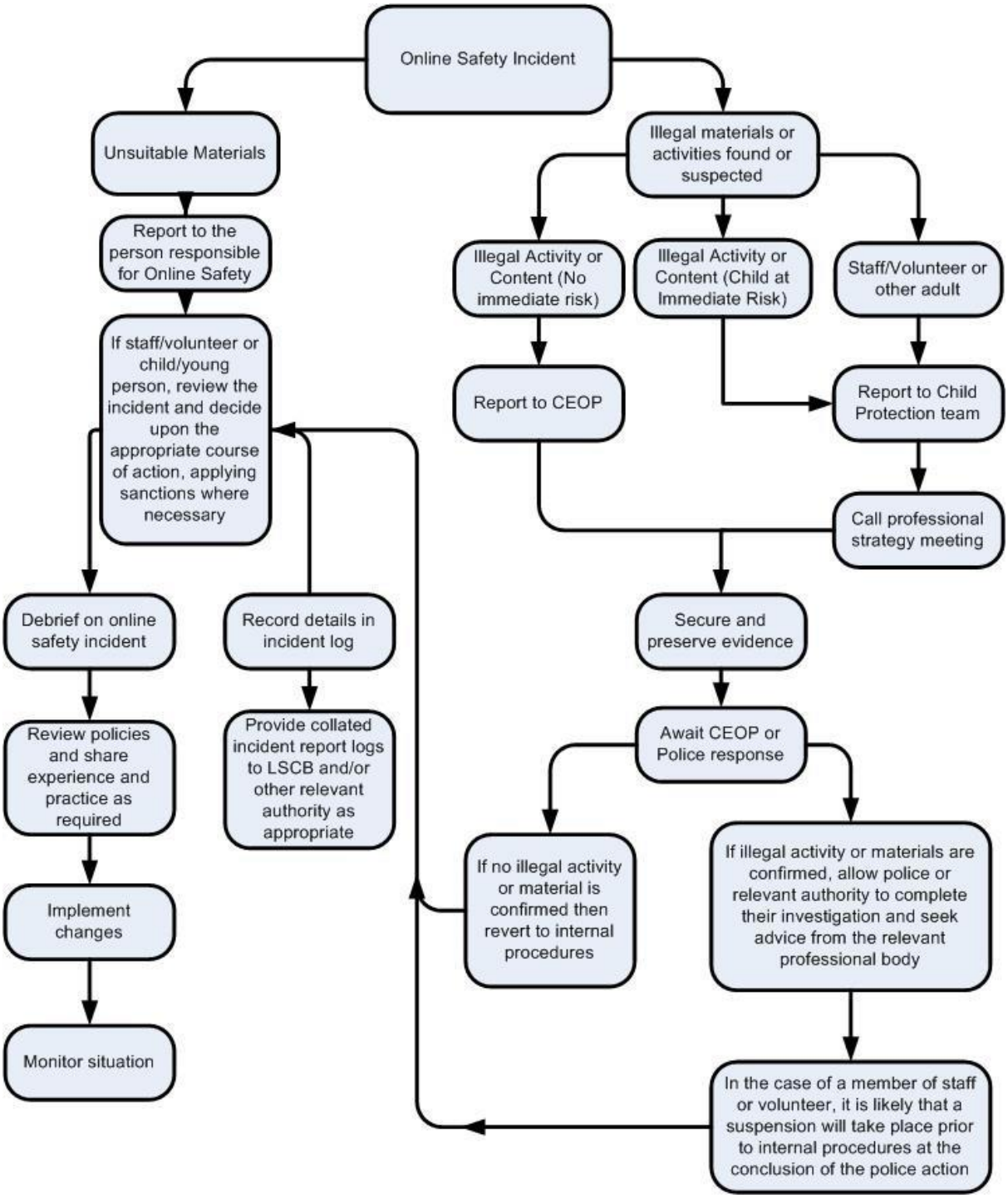
Responding to incidents of misuse

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). Online Safety BOOST includes a comprehensive and interactive

'Incident Management Tool' that steps staff through how to respond, forms to complete and action to take when managing reported incidents (https://boost.swgfl.org.uk/)

Illegal Incidents

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



Other Incidents

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

It is important that all of the above steps are taken as they will provide an evidence trail for the *Federation* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form 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 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:

Actions / Sanctions

Students / Pupils Incidents	Refer to class teacher	Refer to Head of Department / Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction 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	X	X	X	X	X	
Unauthorised use of non-educational sites during lessons	X	X			X			X	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X	X			X	X	X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X	X			X		X	X
Unauthorised downloading or uploading of files	X	X	X		X	X		X	X
Allowing others to access Federation network by sharing username and passwords	X	X	X	X	X	X	X	X	X
Attempting to access or accessing the Federation network, using another student's / pupil's account	X	X	X		X	X		X	
Attempting to access or accessing the Federation network, using the account of a member of staff	X	X	X	X	X	X	X	X	X
Corrupting or destroying the data of other users	X	X	X		X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X	X
Actions which could bring the Federation into disrepute or breach the integrity of the ethos of the Federation	X	X	X		X	X	X	X	X

Using proxy sites or other means to subvert the Federation's filtering system	X	X	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	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X	X

Actions / Sanctions

Staff Incidents	Refer to line managers	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X	X			X	X		X
Allowing others to access Federation network by sharing username and passwords or attempting to access or accessing the Federation network, using another person's account	X	X	X		X	X	X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X	X		X	X	X	X
Deliberate actions to breach data protection or network security rules	X	X	X	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X			X		

Actions which could compromise the staff member's professional standing	X	X	X			X	X	X
Actions which could bring the Federation into disrepute or breach the integrity of the ethos of the Federation	X	X	X	X	X	X	X	X
Using proxy sites or other means to subvert the Federation's filtering system	X	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	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X						
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X

[Type here]