Together Everyone Achieves More

Exhall
Junior School

Online Safety Policy

Adopted by the Governing Body:

Chair of Governors	Signed:	Date: Sept 2022
Head teacher	Signed:	Date: Sept 2022

Date of publication: Dec 2021

Date of next review: Jan 2023

Development / Monitoring / Review of this Policy

This online safety policy has been developed (and will be monitored and reviewed) by a working group:

- Head Teacher
- Senior Leaders
- Online Safety Lead
- Staff – including Teachers, Support Staff & Technical staff
- Governors
- Strategic Advice and Support Service (SAS) through Warwickshire County Council (WCC)
- Parents and Carers

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

Schedule for Development / Monitoring / Review

This Online safety policy was approved by the Governing Body / Governors Sub Committee on:	10/12/21 - ongoing review in light of technology changes
The implementation of this Online safety policy will be monitored by the:	Designated Safeguarding Leads Subject Leader for Computing Online safety representatives
Monitoring will take place at regular intervals:	Reviewed each term or in response to an incident
The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	In the final Head Teacher's report in July. Safeguarding governor(s) will receive monthly reports from the Digital Safeguarding Service.
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:	September 2022
Should serious online safety incidents take place, the following external persons / agencies should be informed:	School Designated Safeguarding Lead(s) Local Authority Safeguarding Lead: Roy Garner Local Authority ICT links: Sarah Fitzgerald / Jane Key

The school will monitor the impact of the policy using:

- Logs of reported incidents through CPOMs and green forms
- Monitoring and filtering logs of internet activity (including sites visited)
- Internal monitoring data for network activity

- Surveys/questionnaires of:
    - Children
    - Parents/carers
    - Staff
- Notes from online safety committee, including the online safety governor and DSLs.

Scope of the policy

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

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

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

Roles and Responsibilities

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

Governors:
Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- Meetings with the Online Safety Lead
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors / Board / committee / meeting

Our Online Safety Governor is: Julia Gaughan

Head Teacher and Senior Leaders:

- The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead / Computing Lead.
- The Head Teacher 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. In the event of the allegation regarding the Head Teacher the Chair of Governors will be informed.
- The Head Teacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head Teacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important

monitoring roles. We currently subscribe to the Local Authority Firewall / Digital Safeguarding Service and monitoring of usage; monthly reports are provided.

Online Safety Coordinator:
Miss Coral Spencer is our Online Safety Lead. She is supported by the Head Teacher, Senior Leaders, Designated Safeguarding Leads and online safety governor who are the designated people for safeguarding. The online safety lead:

- leads the online safety committee
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documentation
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents, forwarded from the Head Teacher
- reports regularly to Senior Leadership Team
- Ensures online safety is taught throughout the curriculum, including remote education.

Technician:
The School's designated Technician is responsible for ensuring:

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

Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Head Teacher or Online Safety Lead for investigation, action and/or sanction
- all digital communications with children / parents / carers / governors should be on a professional level and only carried out using official school systems
- online safety, where necessary, is embedded in all aspects of the curriculum and other activities
- children are aware of the school online safety policy and adhere to acceptable use policies
- children 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, children 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

Children:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school
- Online Safety Ambassadors are a group of children from across the school, that work to support keeping children at Exhall Junior School safe online and meet regularly to provide pupil voice.

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 school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, school website, school social media sites, Virtual Learning Environment (VLE) (for example, Seesaw) and information about national or local online safety campaigns.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Virtual Learning Environment (VLE).

Policy Statements

Education – children:

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

Online safety 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 / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Children should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Children should be helped to understand the need for the pupil Acceptable Use Policy 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 children 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 children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit
- It is accepted that from time to time, for good educational reasons, children may need to research topics (e.g racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technician (or other relevant designated persons) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers:

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

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

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

Education & 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:

- An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies.
- Staff receive online safety training as a part of their GDPR training, that covers IT security. Further online safety training is delivered by the Online Safety Lead and DSL's, during INSET's and Staff Meetings, which shares key messages from their own training.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g from LA and other relevant organisations) and by reviewing guidance documents released by relevant organisations.

- This online safety policy and its updates will be presented to and discussed by staff in staff meetings, INSET days and during Governor meetings.
- The Online Safety Lead (or other nominated person) will provide advice, guidance and training to individuals as required.

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

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation (e.g ICTDS / LA). Note: The online safety governor receives additional training and support.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by *welearn365.com who will keep an up to date record of users and their usernames.* Users are responsible for the security of their username and password
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the *Head Teacher* or other nominated senior leader and kept in a secure place (e.g school safe)
-
- 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.
- 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 / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media 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 (through the school's OneDrive or Google Drive).

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and children 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.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or 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 children are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.
- Permissions are sought for any recorded media in relation remote education.

Communications

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

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

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 *school* / academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to children, parents / carers or school staff

- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and online safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	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	

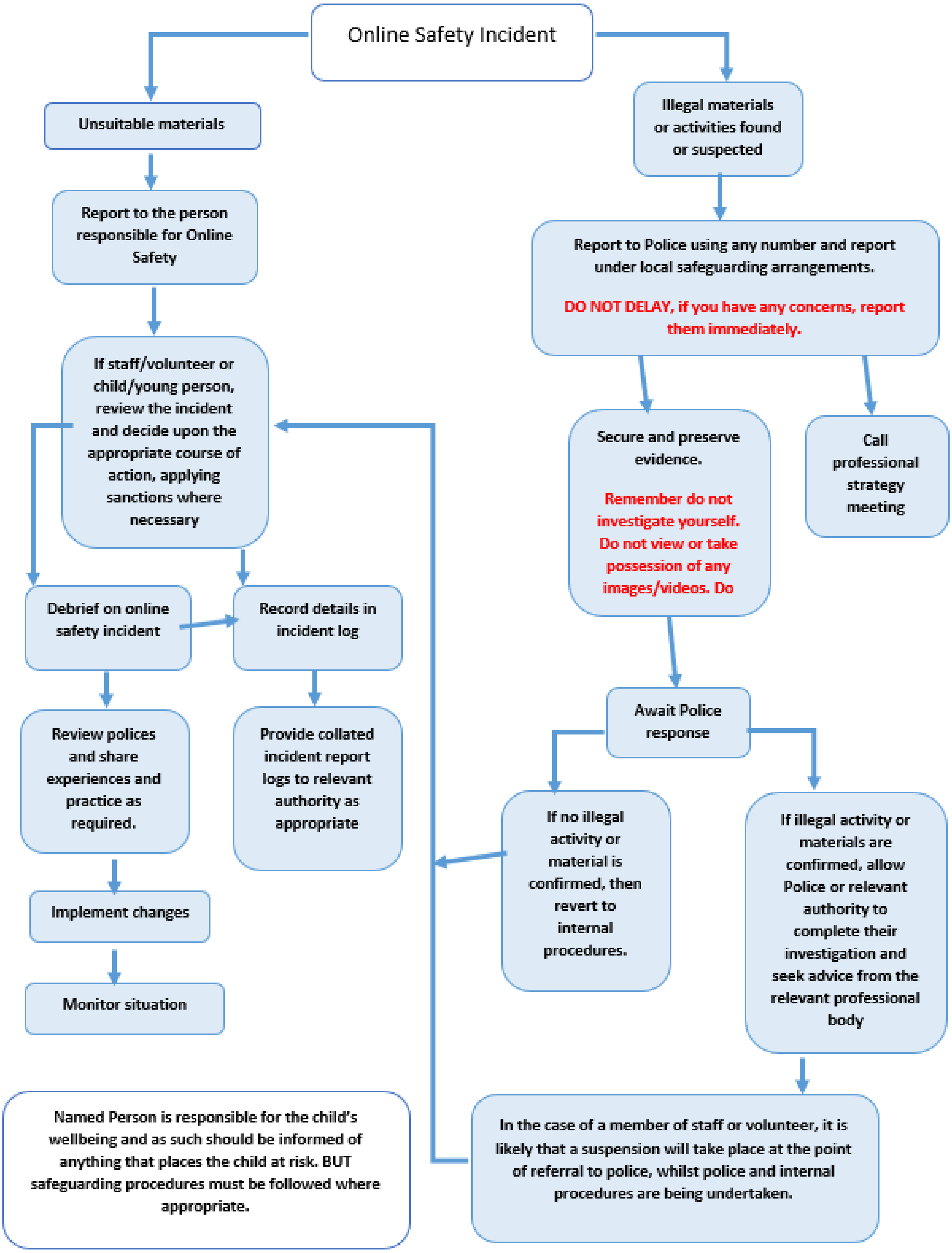
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others 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 website(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 (on the next page) for responding to online safety incidents and report immediately to the police.



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Other incidents:

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

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- 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 school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows (on the next page):

NOTE: Each case will be assessed individually and the action / sanction will be dependent on this.

Children

Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Online Safety Lead	Refer to Head Teacher	Refer to Police	Refer to technical support staff for action re filtering / security	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	x	x					
Unauthorised use of non-educational sites during lessons	X	X	X		X	X	X	X	X
Unauthorised use of mobile phone / digital camera / other mobile device	X	X	X	X		X	X	X	X
Unauthorised use of social media / messaging apps / personal email	X	X	X	X	X	X	X	X	X
Unauthorised downloading or uploading of files	X	X	X	X	X	X	X	X	X
Allowing others to access school / academy network by sharing username and passwords		X						X	X
Attempting to access or accessing the school / academy network, using another student's / pupil's account		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	X	X
Corrupting or destroying the data of other users		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 school into disrepute or breach the integrity of the ethos of the school		X	X			X	X	X	X
Using proxy sites or other means to subvert the school's / academy'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	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

Staff

Actions / Sanctions

Incidents:	Refer to line manager / SLT	Refer to Online Safety Lead	Refer to Data controller / GDPR Lead	Refer to Head Teacher	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				
Inappropriate personal use of the internet / social media / personal email	X	X								
Unauthorised downloading or uploading of files	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	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	X	X	X	X	X	X	X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with children	X	X	X	X	X	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 / academy into disrepute or breach the integrity of the ethos of the school / academy	X	X	X	X						
Using proxy sites or other means to subvert the school's / academy's filtering system	X	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	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	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	X	X	X	X	X

Acknowledgements

Template based on SWGfL online safety policy.