



Westbourne Primary School

Online Safety Policy

To be reviewed in October 2026

SCHEDULE FOR DEVELOPMENT, MONITORING AND REVIEW

This online safety policy was approved by the Trust Board in:	October 2025
The implementation of this online safety policy will be monitored by the:	Designated Safeguarding Leads (Daniel Miracapillo and Claire Mills)
Monitoring will take place at regular intervals:	Annually
The Trust Board will receive a report on the implementation of the online safety policy generated by the online safety co-ordinator 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:	October 2026
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer and CFCS

The school will monitor the impact of the policy using:

- Logs of reported incidents on Google Drive;
- Filtering and monitoring logs;
- Internal monitoring data for network activity;
- Surveys/questionnaires of learners; parents and carers; and staff.

SCOPE OF THE POLICY

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

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

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.

ROLE AND RESPONSIBILITIES

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

TRUSTEES:

Trustees 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 Trustees receiving annual information about online safety incidents and monitoring reports, or more frequently as required. A member of the Trust Board takes on the role of online safety Trustee. The role of the online safety Trustee includes:

- Regular meetings with the Designated Safeguarding Lead;
- Annual monitoring of online safety incident logs;
- Reporting to relevant Trustee meeting;
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible trustee) - in-line with the DfE Filtering and Monitoring Standards.

HEADTEACHER AND SENIOR LEADERS:

- The Headteacher is responsible 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 Designated Safeguarding Leads;
- The Headteacher is responsible for ensuring that the Designated Safeguarding Leads and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant;
- The Senior Leadership Team will receive regular monitoring reports from the Designated Safeguarding Leads;
- The Headteacher and 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 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;
- The Headteacher will receive regular (at least annually) monitoring reports from the Designated Safeguarding Leads;
- The Headteacher will work with the responsible Trustee, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

DESIGNATED SAFEGUARDING LEADS (DSLs)

The DSLs will:

- Hold the lead responsibility for online safety, within their safeguarding role;
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online;
- Meet regularly with the online safety Trustee to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out;
- Report regularly to Headteacher/Senior Leadership Team;
- Be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded;

- Liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety);
- Have a leading role in establishing and reviewing the school online safety policies/documents;
- Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond;
- Treat persistent or unexplained absence as a safeguarding concern. Attendance data will be monitored for patterns that may indicate neglect, exploitation, or other risks, and referrals will be made where appropriate;
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated;
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents;
- Provide (or identify sources of) training and advice for staff/trustees/parents/carers/learners;
- Liaise with external provider technical staff, pastoral staff and support staff (as relevant);
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
 - content
 - contact
 - conduct
 - commerce.

TECHNICAL SUPPORT (supplied by Cygnet in partnership with LGFL):

- Cygnet will ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
- Staff are encouraged to use strong passwords and change their password every 180 days, pupil passwords are securely stored by authorised staff and are changed in bulk whenever a security concern is raised;
- The school uses LGFL filtering system;
- Cygnet 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;
- There is clear, safe, and managed control of user access to networks and devices;

- 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;
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation and action.

TEACHING AND SUPPORT STAFF:

are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters (including online sexual harassment and online sexual abuse), understand it is a core part of safeguarding and are aware of the current school online safety policy and practices;
- They understand that online safety is a core part of safeguarding;
- They have read, understood and signed the school Staff Acceptable Use Policy;
- They report any suspected misuse or problem to the online safety Co-ordinator/Headteacher for investigation;
- Digital communications with pupils and families (e.g. email) should be on a professional level and only carried out using official school systems and ensuring personal data is protected;
- Online safety issues are embedded in all aspects of the curriculum and other school activities;
- The school takes a zero-tolerance approach to incidents of online bullying, sexual harassment, discrimination and hatred;
- That pupils follow the school online safety and acceptable use policy;
- They monitor ICT activity in lessons, extra-curricular and extended school activities;
- They are aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices;
- Where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies;
- 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.

PUPILS:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy;
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- 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.

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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and the school website. Parents and carers will be responsible for:

- Monitoring their child's use of online-enabled devices;
- Be respectful and considerate when using Social Media in relation to the school, and in line with GDPR.

COMMUNITY USERS (the school currently has none):

Before allowing access, community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

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 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 education will be provided in the following ways:

- In line with KCSIE 2025, pupils will be educated about emerging online risks including misinformation, disinformation, and conspiracy theories. These are now recognised as harmful content risks and will be addressed through the online safety curriculum;
- A planned online safety curriculum should be provided as part of Computing/PSHCE lessons, as well as assemblies, and should be regularly revisited;
- Pupils should be taught to be critically aware of 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 should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school;
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices;
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- Where pupils are allowed to 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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

Parents will be informed about new online risks including misinformation and AI through newsletters, workshops, and the school website. Guidance will be provided on how to support children's safe use of technology at home.

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

- Letters, newsletters and the school website;
- Parents evenings/sessions;
- High profile events e.g. Safer Internet Day;
- Reference to CEOP's 'Thinkuknow' website.

EDUCATION AND TRAINING - STAFF

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Annual training will include updates on emerging online risks such as misinformation and AI. Staff will be supported to understand how these risks impact pupils and how to respond appropriately. Training will be offered as follows:

- A planned programme of formal online safety training (annually with regular updates) will be made available to staff;
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies;
- The Online Safety Coordinator will receive regular updates through attendance at training sessions and by reviewing guidance documents;
- This online safety policy and its updates will be presented to and discussed by staff in staff meetings;

- The online safety Coordinator will provide advice, guidance or training as required by individuals.

TRAINING - TRUSTEES

The Trustee with responsibility for Online Safety should take part in online safety training sessions, offered in a number of ways, e.g. specific training courses, information sharing by the Online Safety Co-ordinator and/or DSL.

FILTERING AND MONITORING

The school filtering and monitoring provision is agreed by senior leaders, trustees and Cygnet and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day-to-day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

The filtering and monitoring provision is reviewed (annually) by senior leaders, the Designated Safeguarding Lead and a trustee with the involvement of the IT Service Provider.

The school will use the DfE's 'Plan Technology for Your School' tool to self-assess filtering and monitoring systems annually. Findings will be reported to the Trust Board and used to inform improvements.

Checks on the filtering and monitoring system are carried out by Cygnet with the involvement of a senior leader, the Designated Safeguarding Lead and a trustee, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or new technology is introduced.

Filtering

- The school manages access to content across its systems for all users and on all devices using the LGFL WebScreen Filtering system;
- The school has enabled LGFL Home Protect filtering software on all Chromebooks, should they be taken home by the children (e.g., remote education needs);
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated;
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective;

- There is a clear process in place to deal with, and log, requests/approvals for filtering changes;
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services;
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored;
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention;
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment, including:

- Physical monitoring (adult supervision in the classroom);
- Internet use is logged, regularly monitored and reviewed;
- Filtering logs are regularly analysed and breaches are reported to senior leaders.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- Responsibility for technical security resides with SLT who may delegate activities to identified roles;
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by Cygnet and will be reviewed, at least annually, by the SLT;
- Password policy and procedures are implemented;
- The security of their username and password and must not allow other users to access the systems using their log on details;
- All users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details;
- All school networks and system will be protected by secure passwords. Passwords must not be shared with anyone;

- The administrator passwords for school systems are kept in a secure place;
- There is a risk-based approach to the allocation of learner usernames and passwords;
- There will be regular reviews and audits of the safety and security of school technical systems;
- Servers, wireless systems and cabling are securely located and physical access restricted;
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices 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 endpoint software;
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud;
- Any new software can only be installed by Cygnet technicians as Administrators. Prior to installation, Cygnet will check with a Senior Leader at the school that the software is correctly licenced and can be installed. All new software, including integration systems and apps, are checked for GDPR compliance before installation;
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed;
- Use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network;
- Staff members are not permitted to install software on a school-owned devices;
- Systems are in place to control and protect personal data and data is encrypted at rest and in transit;
- Mobile device security and management procedures are in place;
- Guest users are provided with appropriate access to school systems based on an identified risk profile.

MOBILE TECHNOLOGIES

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

All users should understand that the primary purpose of the use mobile/personal 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 education programme.

- The school Acceptable Use Agreements for staff and pupils will give 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	Yes	Yes	Yes	Yes <i>(written permission required)</i>	Yes	Yes
Full network access	Yes	Yes	Yes		yes	
Internet only						Yes
No network access				Yes		

USE OF DIGITAL AND VIDEO IMAGES – PHOTOGRAPHIC AND VIDEO

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 students / pupils are published on the school 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 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/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 are allowed to take digital/video images of pupils and staff to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes;
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;
- Pupils must not take, use, share, publish or distribute images of others without their permission;
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images;
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs;
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

- 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.

Staff must ensure that they:

- At all times take care to ensure the safekeeping 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, USB stick or any other removable media:

- the data must be encrypted and password protected;
- the device must be password protected (memory sticks / cards and other mobile devices cannot be password protected);
- the device must offer approved virus and malware checking software;
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

COMMUNICATIONS

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				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x							x
Taking photos on personal mobile phones/cameras				x				x
Use of hand-held devices e.g. tablets, gaming devices		x					x	

Use of personal email addresses in school, or on school network		x						x
Use of school email for personal emails				x				x
Use of messaging apps		x						x
Use of social media		x						x
Use of blogs		x					x	

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored;
- Users must immediately report, to a member of Senior Leadership Team – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email;
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE, etc.) must be professional in tone and content;
- Pupils will be provided with individual school email addresses for educational use;
- Students / pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails or messages online.

SOCIAL MEDIA - PROTECTING PROFESSIONAL IDENTITY

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff.

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:

- Ensuring that personal information is not published;
 - Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues;
- School staff should ensure that:
- No reference should be made in social media to students/pupils, 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;
 - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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 school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer (e.g. 'views my own and not of those of school/trust). 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 school permits reasonable and appropriate access to private social media sites

MONITORING OF PUBLIC SOCIAL MEDIA

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school;
- The school will consider how to effectively respond to social media comments made by others;
- When parents/carers express concerns about the school on social media, we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

DEALING WITH UNSUITABLE/INAPPROPRIATE ACTIVITIES

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 certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times (non-working hours)	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
	Promotion of extremism or terrorism					X

	threatening behaviour, including promotion of physical violence or mental harm					X
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LGFL and the school			X			
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					x	

Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				x	
On-line gaming (educational)	X				
On-line gaming (non-educational)		x			
On-line gambling				X	
On-line shopping / commerce		X			
File sharing		X		X	
Use of social networking sites				x	

1.1 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).

1.2 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

1.3 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 Leadership Team member 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.
- Once this has been completed and fully investigated a decision will be made 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 organisation (as relevant).
 - Police involvement and/or action

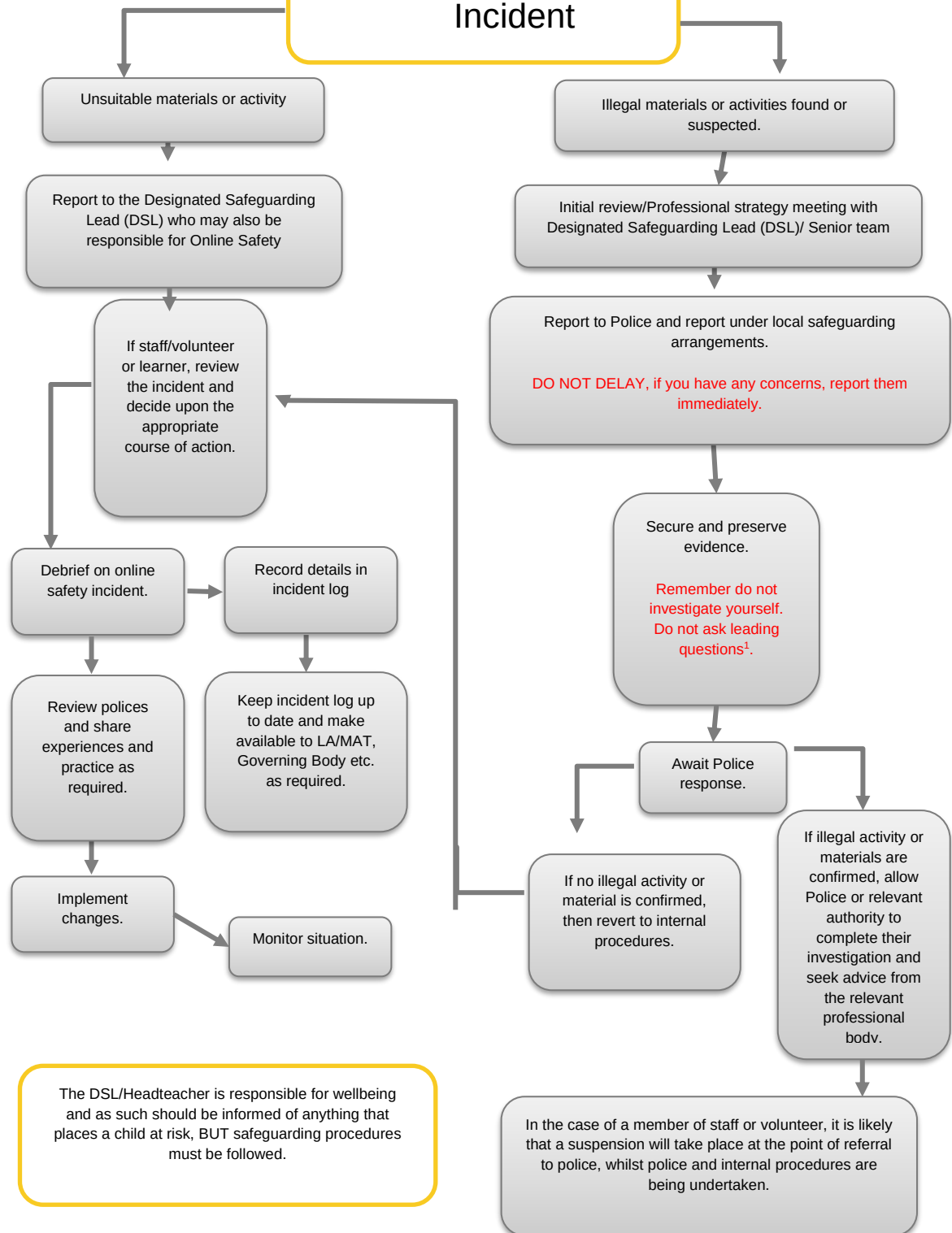
If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police could include:

- 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 school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.

1.1 Online Safety Incident



SCHOOL ACTIONS AND 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:

Students / Pupils	Action/Sanctions						
Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. suspension/ 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
Unauthorised use of non-educational sites during lessons	X					X	
Unauthorised use of mobile phone/ digital camera/other handheld device	X					X	

Unauthorised use of social networking/ instant messaging/personal email	X					X	
Unauthorised downloading or uploading of files	X					x	
Allowing others to access school network by sharing username and passwords	X	x		X	X		
Attempting to access or accessing the school network, using another pupil's account	X	x		X	X		
Attempting to access or accessing the school network, using the account of a member of staff	X	x		X	X		
Corrupting or destroying the data of other users	X	X		X	X		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	x		X	X		
Continued infringements of the above, following previous warnings or sanctions	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
Using proxy sites or other means to subvert the school's filtering system	X	x		x			x
Accidentally accessing offensive or pornographic material and failing to report the incident	X	x		x			
Deliberately accessing or trying to access offensive or pornographic material	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		

Staff

Actions / Sanctions

Incidents:	Refer to performance manager	Refer to Headteacher	Refer to Local Authority	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
Excessive or inappropriate personal use of the internet/social networking sites/instant messaging/personal email		X						X
Unauthorised downloading or uploading of files		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	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner		X			X	X		
Deliberate actions to breach data protection or network security rules		X				x		

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X						X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X				X	X	X
Using personal email/social networking/texting for digital communications with pupils		X						
Actions which could compromise the staff member's professional standing		X				X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X				X	X	X
Using proxy sites or other means to subvert the school's filtering system		X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X	X		
Deliberately accessing or trying to access offensive or pornographic material		X						X
Breaching copyright or licensing regulations		X				X		
Continued infringements of the above, following previous warnings or sanctions		X						X

This is a template – the running log of incidents is saved on the Google Drive

Online Safety Incident Log

(All children found to have behaved inappropriately to have incident added to their ABC log)

[illegible]



Pupil Acceptable Use Agreement

The information below will help children to stay safe online:



- I understand that the school will monitor my use of technology at school and keep me safe online;
- I will only visit internet sites that adults have told me are safe to visit;
- I will treat my username and password like my toothbrush – I will not share it or try to use anybody else's;
- I will be aware of "stranger danger", when I am using the internet and speak to an adult at school if I feel uncomfortable;
- I will not share personal information or images of myself **or others** when online;
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online;
- I will only use school technology for school activities linked to learning;
- I will try not to alter any settings on any devices or try to install any software or programmes;
- I will be polite and responsible when I communicate with others;
- When I am using the internet to find information, I should take care to check that the information that I access is accurate
- I understand that the school can deal with inappropriate online behaviour that takes place out of school, if it affects a person at school.

Signed:



(all children to sign this sheet; it will then be displayed in their classroom)



Staff Acceptable Use Agreement



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

This Acceptable Use Policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

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

Staff must not use generative AI tools with pupils unless approved by SLT and in accordance with school safeguarding protocols.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communication systems.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g., laptops, email, etc.) out of school (e.g., Freedom2Roam VPN).
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person (Headteacher).

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

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

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out

of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

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

(Signed paper copy of the Staff Acceptable Use Agreement in office)