WEST DERBY SCHOOL

ONLINE SAFETY POLICY

This policy will be reviewed:	Annually
Last reviewed:	06/12/2023
Approved on:	16/10/2024
Next review date:	31/12/2025
Approved by:	Trustees Pupil Progress, Achievement and Welfare Committee

Schedule for Development/Monitoring/Review

This Online Safety policy has been developed by a working group made up of: Headteacher, Senior Leaders and Technical staff.

This Online Safety policy was approved by the Trust Board on:	16 October 2024
The implementation of this Online Safety policy will be monitored by:	The Safeguarding Team
Monitoring will take place at regular intervals:	Once a year
The Trust Board will receive a report on online safety incidents at regular intervals:	As per Pupil Progress, Achievement and Welfare Trustees Committee Meetings
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:	Autumn Term 2025
Should serious online safety incidents take place, the following external persons / agencies should be informed:	• Paul Bradshaw, LA Senior School Improvement Officer • Police if necessary
The school will monitor the impact of the policy using:	• Logs of reported incidents • Monitoring logs of internet activity (including sites visited) / filtering • Internal monitoring data for network activity • Surveys / questionnaires of - students - parents / carers

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors) 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 students 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

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 regular information about online safety incidents and monitoring reports.

Headteacher and Senior Leaders:
The Headteacher 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 Designated Safeguarding Lead.

The Headteacher and the Designated Safeguarding Lead are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant disciplinary procedures).

The Headteacher / Senior Leaders are responsible for ensuring that the DSL and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

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

The Designated Safeguarding Lead:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments. meets regularly with Safeguarding Trustee to discuss current issues, review incident logs and filtering / change control logs
- attends relevant committee of Trustees
- reports regularly to Senior Leadership Team

IT Manager / Technical staff

The IT Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack, including patching systems in accordance with NCSC guidelines.
- that the school meets required online safety technical requirements and any guidance that may apply, including that which is set out in the UKCIS guidance, https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords comply with Network complexity requirements and are changed at regular intervals.
- the filtering policies are applied to all users and are regularly updated via Lightspeed Relay's Cloud update system
- 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 is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / DSL for investigation / action / sanction
- that Impero classroom monitoring software is deployed and updated on all network clients
- Sophos Central is deployed to all end user devices, and definition updates are installed as soon as they are released.
- Police Cyber Alarm system is running at all times
- that the IT support staff are kept up to date with all Cyber Security recommendations and requirements from the National Cyber Security Centre (NCSC), this includes annual Cyber Security Training as per RPA 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 complete annual Cyber Security Training
- they have read and understood the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher /DSL for investigation / action / sanction

- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- 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 school 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

Students:

- are responsible for using the school digital technology systems in accordance with the Pupil Network and Internet 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

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 school will take every opportunity to help parents understand these issues through the school. 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
- Their children's personal devices in the school (where this is allowed)

Policy Statements

Education – Students:

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students 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/ PSHE/other lessons and should be regularly revisited

- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students 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
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students 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
- Students 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 and should not use their mobile phones in the vicinity of children unless it is an emergency.
- The school is a mobile phone free zone across Years 7 to 11. Students in the Sixth Form are allowed to use their phones and other devices only during recreational times when in Café West.
- In lessons where internet use is pre-planned, it is best practice that students 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 are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) 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

Keeping Children Safe in Education:

- **All** staff should be aware that technology has become a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content
- The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
- **Content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example per to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images (e.g. consensual or non-consensual sharing of nudes and semi –nudes and / or pornography), and online bullying.

- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If it is felt that pupils or staff are at risk, this should be reported to the Anti-Phishing Working Group (https://apwg.org./)

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

Letters home, school web site, highlighting relevant web sites / publications e.g. swgfl.org.uk; www.saferinternet.org.uk/ and http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers:
It is essential that all staff and volunteers receive online safety training and understand their responsibilities, as outlined in this policy.

- All new staff and volunteers receive Cyber Security Training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy, Cyber and IT security Policy and Acceptable Use Agreements. Online Cyber Security Training is provided alongside the annual safeguarding refresher training for all staff, delivered by the Designated Safeguarding Lead.

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

- Attendance at training provided by the school / Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school / school training / information sessions for staff or parents
- All trustees should complete annual Cyber Security Training

Communications
A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- The official school email/Cloud service (Office 365) 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 school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school 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 school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools 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 liable to the injured party. Reasonable steps to prevent predictable harm are 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:

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

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the 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

When official school social media accounts are established there is/are:

- 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 school 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 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. 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, it is considered good practice to pro-actively monitor the Internet for public postings about the school

- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the DSL or nominated Assistant Headteacher to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The 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 / or outside the school when using school equipment or systems. The school policy restricts usage as follows (please see next page):

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) by nominated persons				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).

Use of digital and video images:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students 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 students 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 are published on the school website / social media / local press

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and UK GDPR which states that personal data must be:

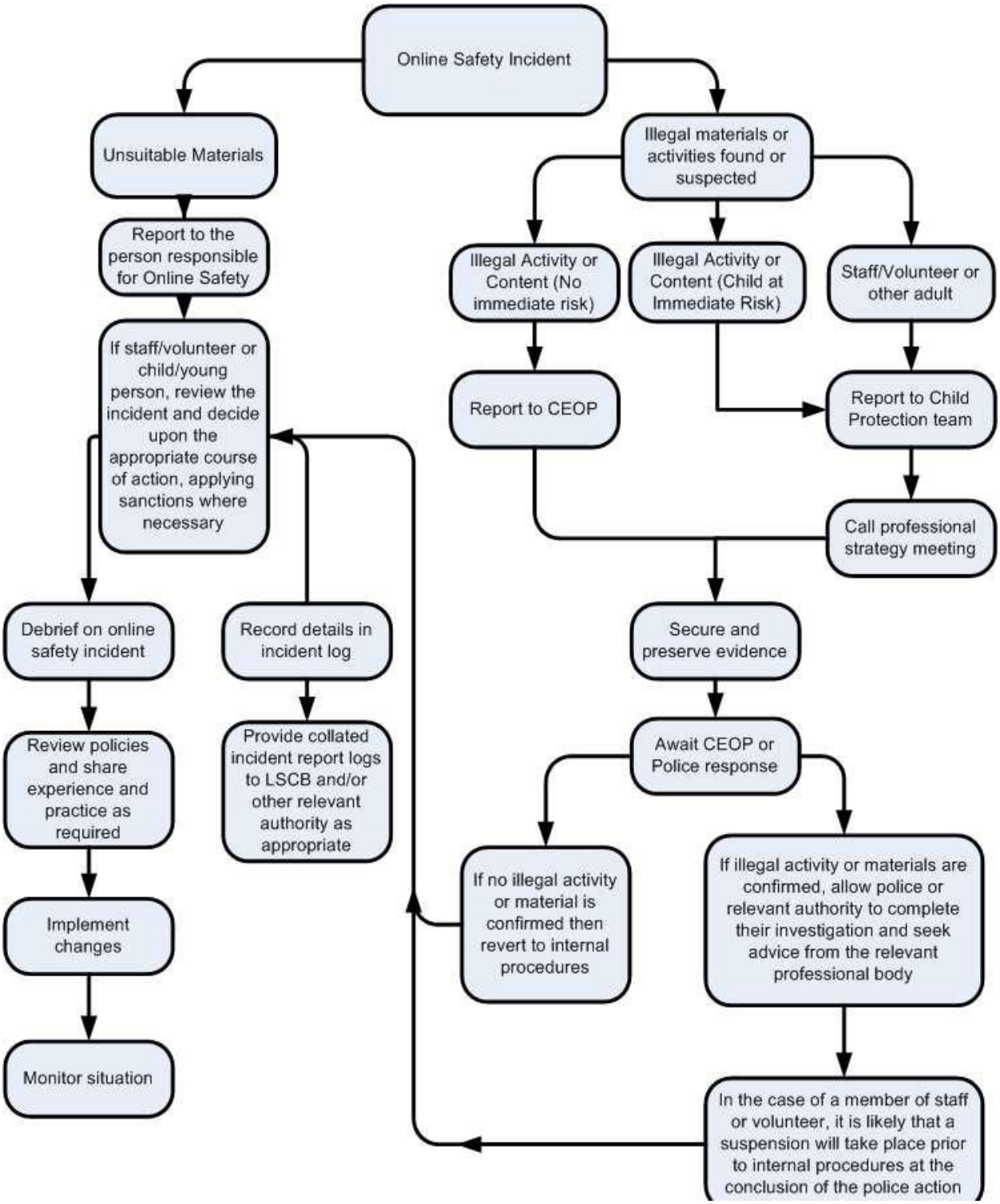
- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school 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 Data Protection Law.

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 Flowchart (below) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
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
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action