DURANTS SCHOOL – POLICY DOCUMENT

E-Safety Policy

Reviewed & updated: February 2024 (Kay Khing)
Next review date: February 2027

CONTENTS

INTRODUCTION

The Internet is managed by a worldwide, non-statutory collaboration of independent agencies that serve mainly an adult audience. Without appropriate measures, access to unsuitable materials would be possible and security compromised. 21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks – to become "Internet Wise". It is Durants School's responsibility to ensure that e-safety reflects the need to raise awareness of internet safety issues.

AIMS

The aims of this e-safety policy are to include but not limited to:

- To protect pupils from undesirable content available on the internet;
- To protect pupils from undesirable contacts over the internet; and
- To prevent unacceptable use of the internet by both pupils and staff.

DEVELOPMENT / MONITORING / REVIEW OF THIS POLICY

This e-safety policy has been developed by a working group made up of:

- Headteacher;
- Senior Leadership Team (SLT);
- School Business Manager; and
- IT Support

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

SCHEDULE FOR DEVELOPMENT / MONITORING / REVIEW

This e-safety policy was approved by Durants School on:	*July 2015*
The implementation of this e-safety policy will be monitored by the:	*Headteacher / SLT / School Business Manager / IT Support*
Monitoring will take place at regular intervals:	*Once every three years at the review date*
The E-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 e-safety or incidents that have taken place. The next anticipated review date will be:	*February 2027*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager / LA Safeguarding Officer / Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents (CPOMS);
- Monitoring logs of internet activity (including sites visited);
- Internal monitoring data for network activity; and / or
- Surveys / questionnaires of:
  - students / pupils;
  - parents / carers; and / or
  - staff.

SCOPE OF THE POLICY

This policy applies to all members of the school community (including staff, students / pupils, 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 students / 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 e-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 e-safety behaviour that take place out of school.

ROLES AND RESPONSIBILITIES

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

GOVERNORS

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. The role of the Governors will include:

- regular meetings with IT Support;
- regular monitoring of e-safety incident logs (CPOMS);
- regular monitoring of filtering / change control logs; and
- reporting to relevant Governors meeting.

HEADTEACHER AND SENIOR LEADERSHIP TEAM

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to IT Support.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Headteacher / Senior Leadership Team are responsible for ensuring that IT Support and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from IT Support.

IT SUPPORT

IT Support 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 e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (if it has one), 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 e-safety technical information in order to effectively carry out their e-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 / attempted misuse can be reported to the Headteacher / Senior Leadership Team / School Business Manager / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

TEACHING AND SUPPORT STAFF

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher / Senior Leadership Team / School Business Manager / IT Support 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
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-safety 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

DESIGNATED SAFEGUARDING LEAD

The DSL should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data

- access to illegal / inappropriate materials

- inappropriate on-line contact with adults / strangers

- potential or actual incidents of grooming

- cyber-bullying

STUDENTS / PUPILS

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so OR be supported by staff in doing so

- will be expected to know and understand policies on the use of mobile devices and digital cameras OR be supported by staff in doing so

- they should also know and understand policies on the taking / use of images and on cyber-bullying OR be supported by staff in doing so

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 parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-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 / VLE and on-line student / pupil records

- their children's personal devices in the school / academy (where this is allowed)

POLICY STATEMENTS

EDUCATION & TRAINING – STAFF / VOLUNTEERS

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

- All staff and volunteers to read, understand, agree and sign the Acceptable Use Policy Agreement

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements

- IT Support will provide advice / guidance / training to individuals as required

USE OF DIGITAL AND VIDEO IMAGES

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

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Students / pupils must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Students' 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 students / pupils are published on the school website

- Student's work can only be published with the permission of the student and parents or carers.

DATA PROTECTION

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

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

The 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 and lawfully processed.
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained

- There are clear and understood policies and routines for the deletion and disposal of data

- There is a policy for reporting, logging, managing and recovering from information risk incidents

- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

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

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

- Transfer data using encryption and secure password protected devices

- When personal data is stored on any portable computer system, memory stick or any other removable media:

    - the data must be encrypted and password protected
    - the device must be password protected
    - the device must offer approved virus and malware checking software
    - the data must be securely deleted from the device, in line with 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:

COMMUNICATION TECHNOLOGIES	STAFF / OTHER ADULTS				STUDENTS / PUPILS			
	Not allowed	Allowed	Allowed at certain times (breaks)	Allowed of selected staff	Not allowed	Allowed	Allowed at certain times (breaks)	Allowed with staff permission
Mobile phones may be brought to school		✓						✓
Use of mobile phones in lessons	✓				✓			
Use of mobile phones in social times			✓					✓
Taking photos on mobile phones / cameras	✓				✓			
Use of other mobile devices, eg tablets etc			✓					✓
Use of personal email addresses in school			✓		✓			
Use of personal email addresses on school network			✓		✓			
Use of school email for personal emails	✓				--	--	--	--
Use of messaging apps			✓		✓			
Use of social media			✓		✓			

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 should be aware that email communications are monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).

- Users must immediately report, to the nominated person – in accordance with the school / academy 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 students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school / academy systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Personal information should not be posted on the school / academy website and only official email addresses should be used to identify members of staff.

SOCIAL MEDIA - PROTECTING PROFESSIONAL IDENTITY

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies 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 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 /academy 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 e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

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 usage as follows:

USER ACTIONS

		Acceptable	Acceptable at certain times	Acceptable for some 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					✓
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					✓
	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					✓
	pornography					✓
	promotion of any kind of discrimination					✓
	threatening behaviour, including promotion of physical violence or mental harm					✓
	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				✓	
Using school systems to run a private business						✓
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					✓	
Infringing copyright						✓
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)						✓
Creating or propagating computer viruses or other harmful files						✓

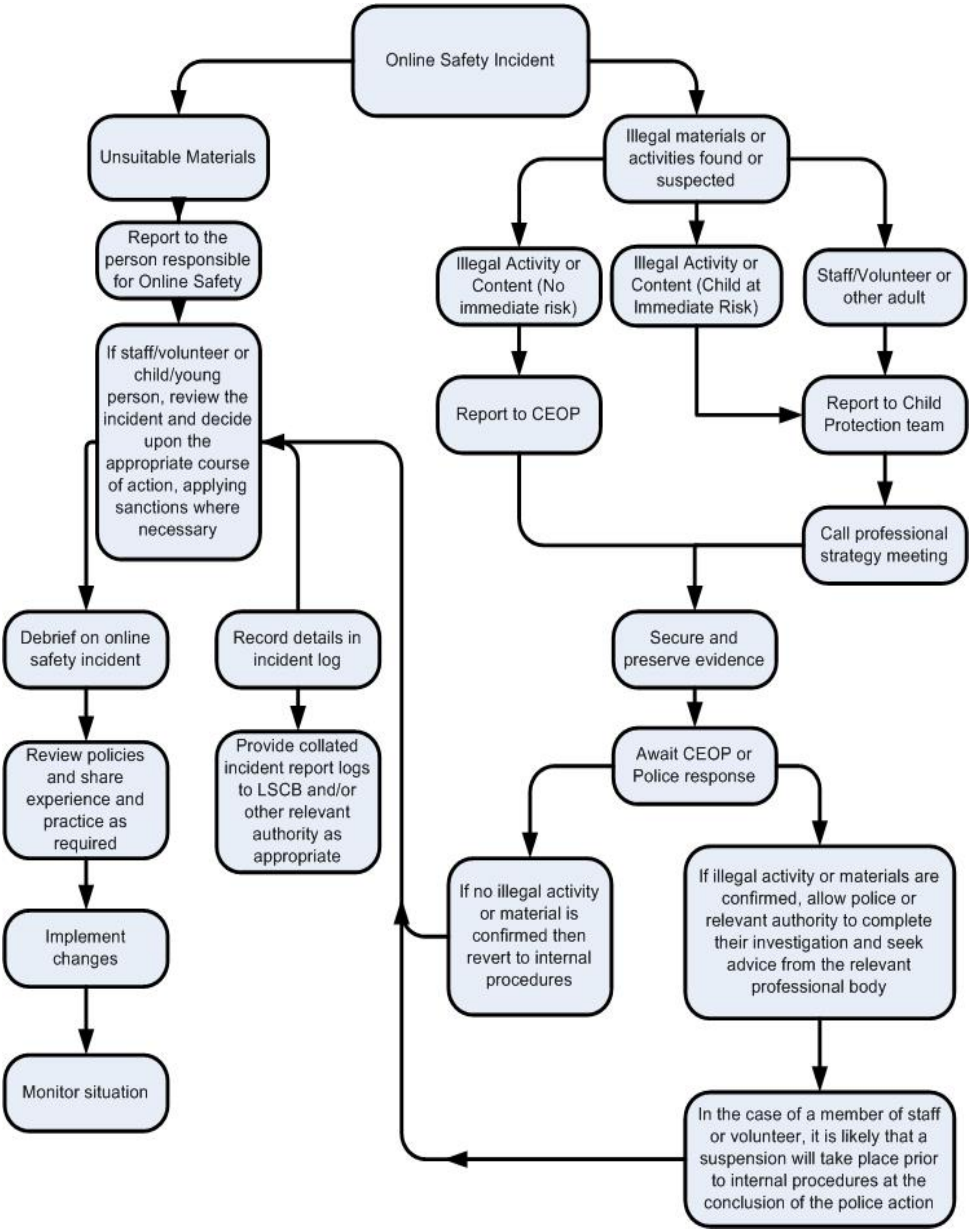
	Acceptable	Acceptable at certain times	Acceptable for some users	Unacceptable	Unacceptable and illegal
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				✓	
On-line gaming (educational)	✓				
On-line gaming (non educational)				✓	
On-line gambling				✓	
On-line shopping / commerce (educational)	✓				
File sharing			✓		
Use of social media		✓			
Use of messaging apps		✓			

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). If a staff member becomes aware of someone participating in illegal or inappropriate activities as listed in the above "User Actions", they should share their concerns with: Headteacher / Senior Leadership Team / School Business Manager / IT Support who will consider what action / sanctions needed to be taken next.

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.


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
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or 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 prior to internal procedures at the conclusion of the police action

Reviewed and updated: February 2024 (Kay Khing)
Next review date: February 2027

OTHER INCIDENTS

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy 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 / academy 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 / academy 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	ACTIONS / SANCTIONS								
INCIDENTS:	Refer to class teacher	Refer to Head of Department	Refer to Headteacher	Refer to Police	Refer to IT Support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓	✓	✓			
Unauthorised use of non-educational sites during lessons	✓				✓	✓		✓	
Unauthorised use of mobile phone / digital camera / other mobile device	✓	✓	✓		✓	✓		✓	
Unauthorised use of social media / messaging apps / personal email	✓	✓			✓	✓		✓	
Unauthorised downloading or uploading of files	✓	✓			✓	✓			
Allowing others to access school / academy network by sharing username and passwords	✓	✓	✓		✓	✓	✓	✓	
Attempting to access or accessing the school / academy network, using the account of a member of staff	✓	✓			✓	✓	✓	✓	
Corrupting or destroying the data of other users	✓	✓	✓		✓	✓	✓	✓	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓				✓		✓	
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓			✓			✓
Actions which could bring the school into disrepute or breach the integrity of the	✓	✓	✓		✓	✓	✓	✓	

STUDENTS / PUPILS	ACTIONS / SANCTIONS								
INCIDENTS:	Refer to class teacher	Refer to Head of Department	Refer to Headteacher	Refer to Police	Refer to IT Support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction
ethos of the school									
Using proxy sites or other means to subvert the school's / academy's filtering system	✓	✓			✓	✓	✓		
Accidentally accessing offensive or pornographic material and failing to report the incident	✓		✓		✓			✓	
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓		✓	✓	✓	✓	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓	✓	✓	✓	✓		

STAFF	ACTIONS / SANCTIONS							
INCIDENTS:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to IT 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).		✓	✓	✓				✓
Inappropriate personal use of the internet / social media / personal email	✓				✓	✓		
Unauthorised downloading or uploading of files	✓				✓	✓		
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	✓	✓			✓	✓		✓
Careless use of personal data eg holding or transferring data in an insecure manner	✓				✓	✓		
Deliberate actions to breach data protection or network security rules	✓	✓	✓	✓	✓			✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓	✓	✓	✓	✓	✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓				✓		✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✓	✓			✓	✓		✓
Actions which could compromise the staff member's professional standing	✓	✓	✓		✓	✓	✓	✓
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	✓	✓	✓		✓	✓		✓
Using proxy sites or other means to subvert the school's / academy's filtering system	✓	✓	✓		✓	✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓				✓	✓		
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓		✓	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓	✓	✓	✓	✓		✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓	✓		✓	✓