Durham Cathedral Schools Foundation

ONLINE SAFETY POLICY

1. Policy Aims

1.1. The purpose of this Policy is to:

- ensure the safety and wellbeing of children and young people are paramount when adults, young people or children are using the internet, social media or mobile devices;
- provide staff and volunteers with the overarching principles that guide our approach to online safety; and
- ensure that, as an organisation, we operate in line with our MARK values and within the law in terms of how we use online devices.

1.2. This Online Safety Policy aims to:

- set expectations for the safe and responsible use of digital technologies for learning, administration, and communication;
- allocate responsibilities for the delivery of the Policy;
- establish how the Policy will be reviewed, taking account of online safety incidents and changes/trends in technology and related behaviours;
- establish guidance for staff and volunteers in how they should use digital technologies responsibly, protecting themselves and the Foundation and how they should use this understanding to help safeguard pupils in the digital world;
- describe how the Foundation will help prepare learners to be safe and responsible users of online technologies; and
- establish clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.

1.3. All children, young people and adults, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

1.4 DCSF commits in this policy to observing the principles of the Equality Act 2010 and does not discriminate on any grounds.

2. Policy Statements

2.1. While DCSF recognises that the online world provides everyone with many opportunities, it can also present risks and challenges. DCSF has a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online. We have a responsibility to help keep children and young people safe online, whether or not they are using DCSF's network and devices, and to work in partnership with children, young people, their parents, carers and other agencies to promote young people's welfare and to help young people to be responsible in their approach to online safety.

2.2. This Policy:

- applies to all members of the DCSF community (including staff, pupils, volunteers, parents/carers, and visitors) who have access to and are users of DCSF digital technology systems, both in and out of the Foundation;
- is supplemented by a series of related acceptable use agreements (see Appendix);
- is made available to staff at induction and on the shared 'common' network drive; and
- is published on the Foundation's website.

2.3. The Education and Inspections Act 2006 empowers the Principal 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 online-bullying or other online safety incidents covered by this Policy and the DCSF Behaviour Policy, which may take place outside of DCSF, but are linked to membership of the Foundation. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

2.4. DCSF will deal with such incidents within this Policy and the associated Behaviour Policy and Anti-Bullying Policy and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

3. Education and Training

3.1. 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/digital literacy is therefore an essential part of DCSF's online safety provision. Children and young people need the help and support of the Foundation 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 is provided as part of Computing/LWE/other lessons and is regularly revisited.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial activities.
- Pupils are taught in all lessons to be critically aware of the materials/content they access online and are guided to validate the accuracy of information (including where the information is gained from AI services).
- Pupils are taught to acknowledge the source of information used and to respect copyright/intellectual property when using material accessed on the internet and particularly through the use of AI services.
- Pupils are 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. The British Values, including mutual respect and tolerance, are emphasised throughout the curriculum.
- Pupils are helped to understand the need for the Pupil Acceptable Use Agreement and are encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- In lessons where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites / tools (including AI services) the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can contact the Deputy Head Pastoral to request that the Network Manager 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.

3.2. 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 children's online 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.

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

- Curriculum activities;
- Letters and monthly Online Safety newsletters;
- Parents/carers evenings/sessions; and
- High profile events/campaigns e.g., Safer Internet Day.

3.3. Education & Training – Staff

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

- A planned programme of formal online safety training is made available to pupil-facing staff. This is regularly updated and reinforced.
- All new staff who have network log-ons receive online safety training as part of their induction programme, ensuring that they fully understand the Foundation's Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the appraisal process.
- The Deputy Head Pastoral as Online Safety Lead will receive regular updates through attendance at external training events (e.g., from the LA and other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings/training sessions.
- The Deputy Head Pastoral, Network Manager and Head of Digital Strategy (or other nominated person) will provide advice/guidance/training to individuals as required.

3.4. Training – Governors

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

- Attendance at training provided by relevant organisations (e.g., National College); and/or
- Participation in DCSF training/information sessions for staff, parents or Governors.

4. Technical – infrastructure/equipment, filtering and monitoring

DCSF is responsible for ensuring that the Foundation's infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this Policy are

implemented. DCSF will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

Key provisions in place are:

- DCSF technical systems will be managed in ways that ensure that the Foundation meets recommended technical requirements, including in the DfE Technical Standards for Schools and Colleges.
- There will be regular reviews and audits of the safety and security of DCSF technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to DCSF technical systems and devices.
- All adult users, and all pupil users from Year 3 and above, will be provided with a username and secure password by the Network Manager, who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- All adult users must use two factor authentication (2FA) when logging into identified programs.
- Appropriate anti-virus software is installed on all Foundation devices.
- Network passwords expire regularly, according to Foundation policies. New passwords must be set on a networked PC.
- Internet access is filtered for all users. Illegal content (e.g., child sexual abuse images) is filtered by Smoothwall, the Foundation's filtering provider, by actively employing the Internet Watch Foundation CAIC list. Smoothwall has provided an acceptable Filtering Provider submission to the UKSIC. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet access in the Foundation's IT rooms is monitored using Impero.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- DCSF has provided enhanced/differentiated user-level filtering, e.g., for staff/pupils, and for certain user groups.
- DCSF technical staff regularly monitor and record the activity of users on the Foundation technical systems and users are made aware of this in the Acceptable Use Agreement. The Deputy Head Pastoral receives instant email alerts of any attempts to access content of very serious concern, and daily email notifications of any attempts to access material online which is categorised as: abuse; suicide; radicalisation; bullying; or criminal activity. The Network Manager sends a copy of the internet filtering log covering all other categories to the Deputy Head Pastoral (also the Online Safety Lead and Designated Safeguarding Lead) on a weekly basis. This is reviewed by the Deputy Head Pastoral and action taken as necessary.
- Staff had training on cyber security in January 2024 and completed an online course on cyber security in September 2025.

- Users report any actual/potential technical incident/security breach to the Head of Digital Strategy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the Foundation's systems and data. These are tested regularly. The Foundation's infrastructure and individual devices are protected by up-to-date virus software.
- An agreed policy is in place for the provision of temporary access of 'guests' (e.g., Governors, visitors) onto the school systems.
- An agreed policy is in place that forbids staff from downloading executable files and installing programs on Foundation devices.
- Care will be taken when using AI services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognize and safeguard sensitive data.
- An agreed policy is in place regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on Foundation devices. **Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured** (see DCSF Data Protection Policy for more details.)

5. Mobile Technologies (including BYOD)

Mobile technology devices may be Foundation owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the Foundation's wireless network. The device then has access to the wider internet which may include cloud-based services such as Office365 which is used for email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices during the school day is educational. The usage of all mobile/personal devices is governed by a range of relevant Foundation polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, and Acceptable Use Agreements. Additional procedures about boarders' use of, and access to, mobile/personal devices outside of the school day are in place for boarders. Teaching about the safe and appropriate use of mobile technologies is an integral part of the Foundation's online safety education programme.

DCSF allows:

	DCSF devices		Personal devices		
	DCSF-owned for single user	**DCSF-owned for multiple users**	**Pupil owned**	**Staff/ volunteer owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	Yes	Yes
Network access	Yes	Yes	No	No	No
Internet only	No	No	Yes	Yes	Yes
No network access	No	No	Yes	Yes	Yes

The use of all devices on the Foundation network is governed by Acceptable Use Agreements.

6. Use of digital and video images

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, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying 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 Foundation will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- A Photography Policy, Photo Management and Storage Process guidance document, a Data Protection Policy, and a Staff and Volunteer Code of Conduct are in place and must be followed by all users.
- As part of the LWE curriculum, and at other relevant times, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they emphasise the risks attached to pupils publishing their own images on the internet, e.g., on social networking sites.
- Pupils understand that they must not take, use, share, publish or distribute images of others without their permission. Breaches of this are dealt with under the Behaviour Policy.

7. Communications

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

	Staff and other adults				Durham School pupils				Chorister School pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile devices may be brought into school	✓				✓					✓		
Use of mobile devices in lessons	✓						✓*				✓	
Use of mobile devices in social time	✓						✓*					✓
Taking photos/videos on mobile devices	✓						✓*				✓	
Use of personal email addresses in school/on school network	✓					✓						✓
Use of school email for personal emails				✓				✓				✓

* Laptops/tablets may be used in this way; mobile phones may not be used during the school day.

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

- The official Foundation email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, in accordance with Foundation 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, etc.) must be professional in tone and content. These communications may only take place on official (monitored) Foundation systems. Personal email addresses, text messaging or social media must not be used for these communications.
- A single network account which is appropriately controlled and monitored may be used for pupils below Year 3, while pupils in Year 3 and above will be provided with individual Foundation email addresses for educational use.
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and are reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the Foundation website and only official email addresses should be used to identify members of staff.

8. Dealing with unsuitable/inappropriate activities

Some internet activity, e.g., accessing child abuse images or distributing racist material is illegal and is obviously banned from Foundation and all other technical systems. Other activities, e.g., cyber-bullying are 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.

DCSF 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 Foundation equipment or systems. This table reflects the fact that some staff and pupils live at school and so may engage in some non-educational activities outside of the school day. DCSF policy restricts usage as follows:

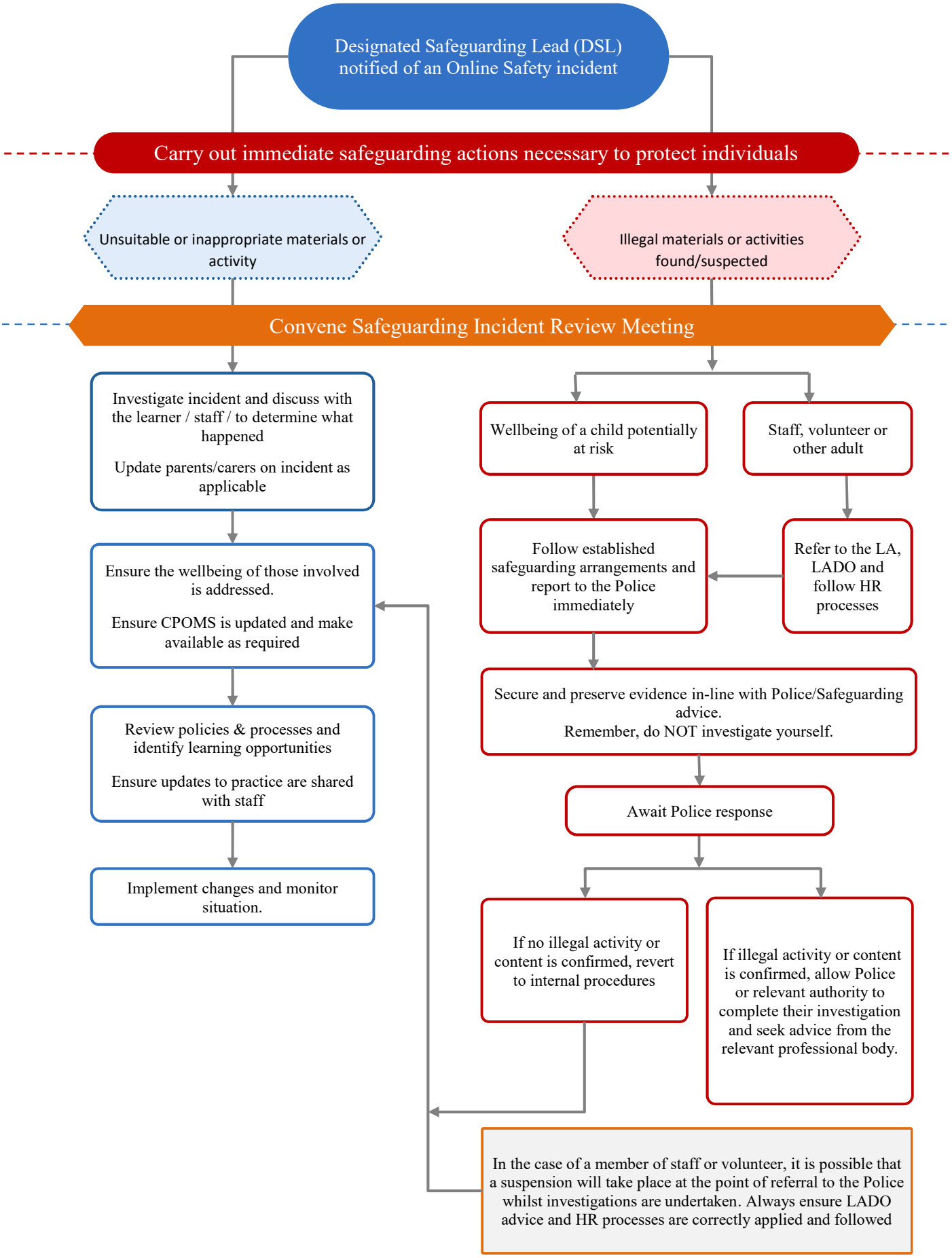
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal	
Users shall not visit internet sites, make, post, download, upload, data transfer, commu-nicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child 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 the 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				✓	✓	
	Promotion of extremism or terrorism				✓	✓	
	Any other information which may be offensive to colleagues or breaches the integrity of Foundation or brings the Foundation into disrepute				✓		

Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					✓
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Foundation				✓	
Revealing or publicising confidential or proprietary information (e.g., financial/personal information, databases, computer/network access codes and passwords)				✓	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			✓	✓	
Using school systems to run a private business				✓	
Infringing copyright and intellectual property (including through the use of AI services)				✓	✓
On-line gaming (educational)	✓				
On-line gaming (non-educational)		✓			
On-line gambling				✓	
On-line shopping/commerce		✓			
File sharing of educational content through approved methods, e.g., Office365	✓				
Use of social media		✓			
Use of messaging apps		✓			
Use of video broadcasting e.g., YouTube		✓			

9. 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). At all times, staff should also have regard to DCSF's Safeguarding Policy and Behaviour Policy.

9.1. Illegal Incidents



9.2. Other Incidents

It is hoped that all members of the Foundation community will be responsible users of digital technologies, who understand and follow Foundation 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 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 pupils 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 and signed (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the Principal 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 of the Local Authority or national/local organisation (as relevant);
    - Police involvement and/or action.
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour;
    - the sending of obscene materials to a child;
    - adult material which potentially breaches the Obscene Publications Act;
    - criminally racist material;
    - promotion of terrorism or extremism;
    - offences under the Computer Misuse Act (see User Actions chart above);
    - 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.**

9.3. Foundation actions and sanctions

It is more likely that the Foundation 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 Foundation 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. The table shows actions which may be taken; not all actions will be taken in response to each incident:

	Actions/Sanctions								
Pupil incidents	Refer to form teacher/SHM	Refer to Deputy Head/DSL	Refer to Headmistress/Principal	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access	Warning	Further sanction e.g., detention in line with Behaviour Policy
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/inappropriate use of mobile phone/digital camera/other mobile device	✓	✓				✓		✓	✓
Unauthorised/inappropriate use of social media/messaging apps/personal email	✓	✓				✓		✓	✓
Unauthorised downloading or uploading of files	✓	✓			✓	✓	✓		✓
Allowing others to access Foundation network by sharing username and passwords	✓	✓			✓	✓			✓
Attempting to access or accessing the Foundation network, using another pupil's account	✓	✓			✓	✓			✓
Attempting to access or accessing the Foundation 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 Foundation into disrepute or breach the integrity or the ethos of the Foundation	✓	✓	✓		✓	✓	✓		✓
Using proxy sites or other means to subvert the Foundation'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/volunteer incidents	Refer to line manager	Refer to Headmistress/Principal*	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	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 Foundation network by sharing username and passwords or attempting to access or accessing the Foundation network, using another person's account	✓	✓			✓	✓
Careless use of personal data e.g., 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 pupils		✓	✓			✓

Actions which could compromise the staff member's professional standing	✓	✓	✓			✓
Actions which could bring the Foundation into disrepute or breach the integrity or the ethos of the Foundation	✓	✓	✓		✓	✓
Using proxy sites or other means to subvert the Foundation'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/intellectual property or licensing regulations (including through the use of AI services)	✓	✓			✓	✓
Continued infringements of the above, following previous warnings or sanctions		✓			✓	✓

* any concern about misuse involving the Principal should be referred to the Chair of Governors.

10. Responsibilities

10.1. Governors

The DfE's *Keeping Children Safe in Education* (September 2025) says:

> Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement. (Paragraph 136) …
>
> governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system and the proportionality of costs versus safeguarding risks. (Paragraph 140)

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the Policy. This will be carried out by the Governors receiving information about online safety incidents and monitoring reports at termly Full Board meetings. The Safeguarding Governor will be informed of any online safety incidents which involve child protection concerns. Online safety may also be discussed at Governor Sub-Committee meetings as appropriate, e.g., Health, Safety and Welfare; Finance and General Purposes etc.

10.2 Headmistress/Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the Foundation community, though the day-to-day responsibility for online safety will be delegated to the Deputy Head Pastoral.
- The Headmistress and Principal 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 Headmistress/Principal and Senior Leaders are responsible for ensuring that staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive monitoring reports from the Deputy Head Pastoral as appropriate.

10.3 Deputy Head Pastoral

The Deputy Head Pastoral is the named member of staff with a day-to-day responsibility for online safety. Their role is to:

- take day-to-day responsibility for online safety issues and have a leading role in establishing and reviewing the Foundation's online safety policies/documents;
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- provide/source/arrange training and advice for staff as necessary;
- liaise with the Local Authority, police and any other relevant bodies;
- liaise with Foundation technical staff;
- receive reports of online safety incidents and create a log of incidents on CPOMS to inform future online safety developments;
- liaise with Safeguarding Governor to discuss current issues, review CPOMS logs and filtering/change control logs;
- attend relevant meetings of Governors;
- report regularly to the Senior Leadership Team.

As the Designated Safeguarding Lead, the Deputy Head Pastoral should also 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;

- online-bullying.

10.4 Head of Digital Strategy, Network Manager and other technical staff

Those with technical responsibilities are responsible for ensuring:

- that the Foundation's technical infrastructure is secure and is not open to misuse or malicious attack;
- that the Foundation meets required online safety technical requirements and any other online safety policy/guidance that may apply;
- that users may only access the networks and devices through a properly enforced password protection policy;
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- that the use of the Foundation network/internet is regularly monitored in order that any misuse/attempted misuse can be reported to the Deputy Head Pastoral for investigation/action/sanction;
- that monitoring software/systems are implemented and updated as agreed in school/academy policies.

10.5 Teaching and Support Staff

Are responsible for ensuring that:

- they attend online safety training as instructed and have an up-to-date awareness of the Foundation Online Safety Policy and practices;
- they have read, understood and signed the staff Acceptable Use Agreement;
- they understand that online safety is a core part of safeguarding;
- they report any suspected misuse or problem to the Deputy Head Pastoral or Principal as appropriate for investigation/action/sanction;
- all digital communications with pupils/parents/carers are on a professional level and only carried out using official school systems. Where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organizational security and oversight requirements;
- they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education (September 2025) and UK GDPR regulations;
- online safety issues are embedded in all aspects of the curriculum and other activities;
- as appropriate to their age, pupils understand and follow the Online Safety Policy and acceptable use policies;
- as appropriate to their age, 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, 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies;
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.;
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media;
- they adhere to the Foundation's technical security policy, with regard to the use of devices, systems and passwords, and have an understanding of basic cybersecurity;
- they are aware of the benefits and risks of the use of AI services in school, being transparent in how they use these services, prioritizing human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

10.6 Pupils

As appropriate for their age and ability, pupils:

- are responsible for using the Foundation's digital technology systems in accordance with the pupil Acceptable Use Agreement;
- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. When using AI services, they should take care to protect the intellectual property of themselves and others, and check the accuracy of content accessed through AI services;
- 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 online-bullying;
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Foundation's Online Safety Policy covers their actions out of school, if related to their membership of the Foundation.

10.7 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 Foundation will take every opportunity to help parents/carers understand these issues through:

- publishing the Online Safety Policy on the Foundation's website;
- providing them with a copy of the learners' acceptable use agreement;
- making available information about appropriate use of social media relating to posts concerning the school;
- seeking their permissions concerning the use of digital images, cloud services, etc.;

- parents'/carers' evenings, monthly Online Safety newsletters, publication on the DCSF website and social media information about national/local online safety campaigns and literature.

Parents/carers will be encouraged to support the Foundation 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 on-line pupil records;
- their children's personal devices.

11. Cross reference to other policies and documents

This Policy is linked to the following policies and documents:

- Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff and Volunteer Code of Conduct
- School Rules [Durham School]
- Searching a Pupil Room or Property Policy
- BYOD Policy and Acceptable Use Agreements
- Remote Learning Policy
- External Communication Policy
- Data Protection Policy
- Data Retention Guidelines
- Photography Policy
- Guest Wireless Terms and Conditions of Use
- Photo Management and Storage Process
- Provision of Access to Online Materials by Pupils
- Relationships and Sex Education (RSE) Policy

12. Oversight

Oversight of this Policy is undertaken by the Education Committee of the Governing Body, and the Policy will be reviewed annually.

Policy reviewed by
Harriet Thompson, Deputy Head Pastoral, on 21 September 2025
Harriet Thompson, Deputy Head Pastoral, on 26 October 2024
Harriet Thompson, Deputy Head Pastoral, on 1 November 2023
Policy written by
Harriet Thompson, Deputy Head Pastoral, on 1 November 2022