E-Safety Policy

Ellesmere College

E-Safety Policy Statement

The College's E-Safety Policy complies with the Statutory Guidelines KCSE 2024, Meeting Digital and Technology Standards in Schools and Colleges, March 2022 (updated March 2023). This policy acknowledges the guidance provided by '360 Degree Safe', the E-Safety self-review tool provided by the South West Grid for Learning Trust - SWGfL.

The purpose of the policy is to provide a framework within which the school community can benefit from the advances in internet and other communication technologies whilst protecting users from misuse and harm.

1. Leadership and responsibility

The wider school community has a responsibility to act in such a way as to protect others from misuse of technology. Leadership will be provided by the E-Safety Committee (ESC), the members of which will represent the SMT, employees, governors and pupils. The committee is responsible to the Headmaster.

E-Safety Committee: the committee will be composed of:

- Chairman and member of the SMT: Deputy Head Pastoral
- Member of SMT with responsibility for IT and CPO: Deputy Head Academic
- Head of Lower School
- Head of Middle School
- Head of Sixth Form
- Director of ICT
- Head of Computer Science
- Governor representative
- Pupil representatives, at least one day pupil and one boarder pupil.

The Committee will meet once per term.

2. Policy scope

The policy covers the use of the ICT systems, equipment and software in school and addresses issues related to the use of school related ICT out of school. It also covers the use of personal ICT equipment both in school and out of school (where use can be considered to have a bearing upon the good name of the school or the wellbeing of the members of its community).

3. Acceptable use policies

There are acceptable use policies for both employees / adult volunteers (see IT Network & Internet AUP (Staff) **Appendix 1**) and for pupils. Parents are acknowledging that they have read the AUP's when they sign their acceptance documents and terms and conditions. Parents of pupils joining the school receive information and, as part of their terms and conditions, sign to say they have read the AUP. When pupils move up from Lower School to Middle School and from Middle School to Sixth Form they are asked to re-sign the AUP (see Agreement of Use: IT Network & Internet AUP (Pupils & Parents) **Appendix 2**). Tutors go through the E-Safety Information Checklist (**Appendix 3**) with pupils at the start of each new academic year (the copies will be kept on file).

4. Links with other policies

The E-safety policy (ESP) should be read in conjunction with, and taken to include the provisions of, the following school policies: Child protection and safeguarding, Anti-bullying, Defamatory information, Data Protection, Mobile phone and smart technology, Personal Data, PSHE and the Complaints policy.

5. Sanctions and rewards

Sanctions for failing to adhere to the ESP are in line with those outlined in the linked policies and defer to them except where an alternative sanction is mentioned. It should be noted that all sanctions are at the Headmaster's discretion although those mentioned are normally the minimum sanction that may be expected. Public spirited actions promoting the sensible use of the technology, improvements to systems and the avoidance of harm or distress to others may be rewarded in line with the school Rewards and Sanctions Policy.

6. Reporting and monitoring

It is a requirement of the AUP's that users report any incidents of abuse, worries about actual, potential or perceived e-safety incidents to a member of Common Room (CR) who will, in turn, inform a CR member of the ESP committee (ESC). Reports will be logged by the Secretary and will be audited and monitored by the Chairman of the ESC at least annually. Parents and carers will be informed of e-safety incidents involving young people for whom they are responsible and of significant patterns of e-safety incidents. The reporting and monitoring of incidents will contribute to the development of e-safety policy and practice.

7. Filtering and monitoring

The school's internet service is provided by a fully credited ISP and accredited filtering is in place. The school has provided enhanced user level filtering. Monitoring (through Imperio) compliments the filtering and breaches of the filtering policy are reported to the Secretary of the ESC who will discuss and manage any necessary changes through the Director of ICT

7.1

- Deputy Head Academic is responsible for SMT oversight
- Director of ICT manages the day to day filtering and monitoring systems
- The filtering and monitoring system is reviewed annually (Appendix 5)
- Harmful and inappropriate content is blocked without unreasonably impacting teaching and learning
- Effective monitoring strategies are in place and include:
    - Physically monitoring by staff watching screens of users
    - Live supervision by staff on a console with device management software
    - Network monitoring using log files of internet traffic and web access
    - Individual device monitoring through software or third-party services
    - Governors are on the E-Safety Committee and are therefore able to review standards and discuss with ICT staff to make sure the filtering and monitoring standards are met

7.2 All staff should report if:

- They witness or suspect unacceptable material has been accessed
- They can access unsuitable material
- They are teaching content that could cause spike in logs
- There is failure in the software or abuse of the system
- There are perceived unreasonable restrictions
- They notice abbreviations or misspellings that allow access to restricted material

7.3 The filtering system blocks:

- Illegal child sexual abuse
- Unlawful terrorist content
- Adult content
- Content deemed harmful to children

8. Technical security

The school ICT infrastructure is reviewed on a regular basis by the Director of ICT to ensure that it is not open to misuse or malicious attack.

9. Volunteers

Volunteers should not have access to school based ICT systems that may involve personal or sensitive information.

10. Education

E-safety education takes place through PSHE/Computer Science/and other lessons across the curriculum. In particular, all years follow and complete the Online Safety Alliance Course. The school considers the vulnerability of pupils due to age or other circumstances, like SEND when considering the risk due to their own or others actions on line or via other systems. The impact and effectiveness of the e-safety programmes are monitored and evaluated by the ESC.

11. Information literacy

Areas of the curriculum teach pupils to be critically aware of the material and content that they access on line and they are guided to attempt to validate the accuracy of information. Research skills, the need to avoid plagiarism and the upholding of copyright regulations are emphasised where appropriate.

12. Staff training

Training in e-safety is closely linked to that for safeguarding / child protection and it is College policy that all staff should attend 'Raising awareness in safeguarding and child protection', a course certificated by Shropshire Safeguarding Board. The E-safety Committee will distribute information and / or arrange in-service training as felt necessary.

13. Governor information

E-safety information is provided for Governors and a nominated Governor is a member of the ESC, reporting back to the School Council.

14. Parental education

The school provides opportunities for parents to receive education or information about e-safety through briefings at some parents' meetings, newsletters, the college website, 'Parent mail' or other communications. Parents and carers are aware of and endorse the pupil AUP and are provided with contact details should they be worried about e-safety issues or wish to enquire or make a complaint.

15. Other information

15.1 E-Safety Information Leaflet (**Appendix 4**), available on Ellesmere College website.

15.2 National Online Safety - Guides for Parents

To help parents navigate the many social media sites, apps, games, and messaging apps now available on the internet and through mobile devices, and to provide support in general for internet use, etiquette and safety, we have teamed up with National Online Safety - an organisation who work with schools and school staff, parents and children, equipping them with the knowledge they need to understand online dangers and how best to react should an incident arise and ultimately to make the internet a safer place for children.
https://www.ellesmere.com/pastoral/college-policy-documents

15.3 Appendix 5 gives a check list for meeting Digital and Technology Standards in School (Andrew Hall). This is part of the annual review.

15.4 Appendix 6 is the UK Safer Internet Central Filtering and Monitoring Checklist Register that is being used.

16. Review

The annual review of this policy will be undertaken by the Deputy Head Pastoral who will take into account any guidance published by the DfE and ISI.

Authorised by	Headmaster
Date	September 2024
Reviewed by	Deputy Head Pastoral
Date	September 2024

APPENDIX 1:

IT Network & Internet Acceptable Use Policy (Staff)

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Deputy Head Pastoral (DHP) or Deputy Head Academic (DHA).

- I will only use the College's email, internet, intranet, learning platform and any related technologies for professional purposes or for uses deemed 'responsible' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the College or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will consider the possible ramifications of giving out my own personal details, such as mobile phone number and personal email address, to pupils and will not do so except for approved reasons.
- I will only use the approved, secure email system(s) for any College business and not use it for personal business.
- I will ensure that personal data (such as data held on SIMS software) is kept secure and is used appropriately, whether in College, taken off the College premises or accessed remotely. Personal data can only be taken out of College or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without the knowledge of the Director of ICT.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and / or staff will only be taken, stored and used for professional purposes in line with College policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the College network without the permission of the Headmaster.
- I will support the College's approach to on-line safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the College community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headmaster. I will respect copyright and intellectual property rights.
- I will ensure that my on-line activity, both in College and outside College, will not bring my professional role into disrepute.
- I will follow, support and promote the College's E-Safety and Information Security Policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand that I have a duty to report misuse of the College's systems to the DHA or DHP.

IT Network and Internet Acceptable Use Policy – User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the College.

Full Name of Member of Staff (please print): _____

Signature: _____ Date: _____

APPENDIX 2:

Agreement of use: IT Network and Internet (Pupils and Parents)

R. Chatterjee, PhD.
Deputy Head Pastoral
ranjit.chatterjee@ellesmere.com

Date

Dear Parent,

E-Safety IT Policy Agreement

ICT including the internet, email, mobile technologies and online resources have become an important part of learning in the school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of e-safety and know how to stay safe when using any ICT. On joining the College you read and signed the E-Safety Agreement, but as your child now moves into either Middle School or the Sixth Form (and with the advances in technology) it is prudent to send out a reminder.

Pupils are expected to read and discuss the attached E-Safety IT Policy agreement with their parent/guardian and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their tutor or the Head of Middle School or Sixth Form as appropriate.

Please return the bottom section of this form to school for filing.

Yours sincerely,

Enc.

✂

IT Network and Internet Acceptable Use Policy, Pupil and Parent/ Guardian signature

We have discussed this document and ***(pupil name)***: _____

agrees to follow the e-Safety rules and to support the safe and responsible use of ICT at Ellesmere.

Parent/Guardian Signature: _____ Date: _____

Pupil Signature:_____ Date: _____

Agreement of use: IT Network and Internet – Pupils and Parents

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school or appropriate social purposes. ('Appropriate' means both in terms of content and location and time of access.)
- I will not download or install software on school IT devices.

- I will only log on to the school network, other systems and resources with my own user name and password.
- I will follow the school's ICT security policy and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address for school purposes.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of the College staff.
- I will not give out any personal information such as name, phone number or address unless for authorized school purposes. I will not use an on-line facility to meet someone.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of The Headmaster.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school or anyone else into disrepute, for example *Facebook*.
- I will respect the privacy and ownership of others' work on-line at all times. (I will not claim others' work as my own recognising plagiarism and copyright).
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ guardian may be contacted.
- I understand that I have a duty to report misuse of the school's ICT systems to a member of College staff.
- I will abide by appropriate age related guidelines, e.g. Facebook, Snapchat, etc.

APPENDIX 3:

E-SAFETY CHECKLIST FOR PUPILS

(To be explained by Tutors and signed for at the start of each new academic year or when joining the College.)

E-Safety IT Policy Agreement

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school or appropriate social purposes. ('Appropriate' means both in terms of content and location and time of access.)
- I will not download or install software on school IT devices.
- I will only log on to the school network, other systems and resources with my own user name and password.
- I will follow the school's ICT security policy and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address for school purposes.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of the College staff.
- I will not give out any personal information such as name, phone number or address unless for authorized school purposes. I will not use an on-line facility to meet someone.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of The Headmaster.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school or anyone else into disrepute, for example *Facebook*.
- I will respect the privacy and ownership of others' work on-line at all times. (I will not claim others' work as my own recognising plagiarism and copyright).
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ guardian may be contacted.
- I understand that I have a duty to report misuse of the school's ICT systems to a member of College staff.
- I will abide by appropriate age related guidelines, e.g. Facebook, Snapchat, etc.

Please complete the following table:

Please respond to the following questions	Your response:
If you felt uncomfortable about anything that you saw, or if anyone asked you for your personal details, such as your address and age on the internet, would you know where to go to get help?	Please say what you would do:
If anybody sent you hurtful messages on the internet or on your mobile phone, would you know who to tell?	Please say who you would tell:
Do you understand what the risks of posting inappropriate content on the internet are? (Senior School pupils only)	List some of the risks here:

I have discussed this document with my tutor and have answered any questions I may have related to safety on-line.

Pupil signature: _____ Date: _____

This document has been discussed with the pupil and any questions they may have answered.

Tutor signature: _____ Date: _____

APPENDIX 4:

E-SAFETY INFORMATION LEAFLET

There is evidence of the mismatch between the high technical abilities of pupils as users of electronic devices and their low awareness of safety issues involved. This was geographically illustrated in a report in 'The Independent' on a survey of 1000 girls aged between 10 and 18, which stated that:

"Almost half of the girls had seen things online which upset or frightened them. More than one in four had been bullied on the internet and a fifth had considered meeting someone they met online in real life, although a similar number said they had found people who were not who they said they were….. Almost all girls (95%) believed carrying a mobile phone makes them safer, unaware of the risks of displaying valuables. Nearly 80% of girls aged 16 to18 listen to an iPod while walking alone at night".

57% of parents do not know where to go to get information on how to protect their children online.

ICT IN THE CURRICULUM

All of Ellesmere's pupils are taught how to research on the internet and to evaluate sources. They are educated into the importance of evaluating the intellectual integrity of different websites and why some apparently authoritative sites need to be treated with caution. Some websites masquerade as serious, impartial, historical sites but are actually sources of racist, homophobic, jihadist or other propaganda.
Some free, online encyclopaedias do not evaluate or screen the material posted on them.

THE ROLE OF TECHNOLOGY IN OUR PUPILS' LIVES

Technology plays an enormously important part in the lives of all young people. Sophisticated games consoles, or PSP's (play stations portable), like Wii's and Nintendo DS, together with Bluetooth-enabled mobile phones provide unlimited access to the internet, to SMS messages, to blogging (web logging), to social media websites (like Twitter), to Skype (video calls, via web cameras built into computers, phones and PSP's), to wikis (collaborative web pages), chat rooms and other social networking sites (such as Bebo, Facebook and MySpace), and video sharing sites (such as YouTube). This communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of the school's role to teach pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking, abuse and exposing themselves to subsequent embarrassment.

ROLE OF OUR TECHNICAL STAFF

Ellesmere attempts to teach all of its pupils to understand why they need to behave responsibly to protect themselves. The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its software and data and for aspects of training the school's teaching and administrative staff in the use of ICT. They monitor the use of the internet and emails and will report inappropriate usage to the pastoral staff.

ROLE OF OUR CHILD PROTECTION OFFICER AND THE E-SAFETY COMMITTEE

Ellesmere recognises that internet safety is a child protection and general safeguarding issue. The E-Safety Committee, chaired by the CPO, will seek to ensure that relevant information is made available to pastoral staff, promoting training where considered necessary, and will oversee the education of pupils and the provision of information to parents. It is the responsibility of the CPO to handle allegations of misuse of the internet.

MISUSE: STATEMENT OF POLICY

Ellesmere will not tolerate any illegal material and will involve the police and/or the LSCB where necessary. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our anti-bullying policy.

INVOLVEMENT OF PARENTS AND GUARDIANS

The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will fee able to share any concerns with the school. The school recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. The school will occasionally provide information regarding potential hazards of this exploding technology and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity. This leaflet provides basic information for the awareness of parents.

CHARTER FOR THE SAFE USE OF THE INTERNET AND ELECTRONIC DEVICES AT ELLESMERE COLLEGE

E-Safety is a whole school responsibility and the staff and pupils have adopted the following charter for the safe use of the internet inside the school:

Cyber-bullying

- Cyber-bullying is a particularly pernicious form of bullying because it can be so pervasive and anonymous. There can be no safe haven for the victim who can be targeted at any time or place. The school's anti-bullying policy describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying.
- Proper supervision of pupils plays an important part in creating a safe ICT environment at school, but everyone needs to learn how to stay safe outside the school.
- It is part of the ethos of the school to promote considerate behaviour and to value diversity.
- Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to come forward.

Treating Other Users with Respect

- The school expects pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face to face contact.
- The school expects a degree of formality in communications between staff and pupils and would not normally expect them to communicate with each other by text or mobile phones unless the member of staff were to use an official school mobile phone or the communication was known to and sanctioned by one of the Deputy Heads.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The school's anti-bullying policy is available on the school's website. All pupils are encouraged to look after each other and to report any concerns about the misuse of technology or worrying issue to a member of the pastoral staff.

Keeping the School Network Safe

- Certain sites are blocked by the school's filtering system and the school's IT department monitors pupils' use of the network, email traffic, and blocks SPAM and certain attachments.
- The school issues all pupils with their own personal school email address. Access is via personal LOGIN, which is password protected. (Passwords are personal and should never be shared).

- The school has strong anti-virus protection on its network which is operated by the IT department.
- Any member of staff or pupil who wishes to connect a removable device to the school's network should note that the school's software will check it for viruses and may not permit connection.

Promoting Safe Use of Technology

Parents and pupils of all ages are encouraged to make use of the excellent online resources that are available from sites such as:

- UK Council for Child Internet Safety (http://www.education.gov.uk/ukccis)
- Childnet International (www.childnet-int.org)
- Cyber Mentors, for young people, trained mentors on line (www.cybermentors.org.uk)
- Cyber-bullying (www.cyberbullying.org)
- Bullying UK (www.bullying.co.uk)
- CEOPS educational section, a good first port of call (https://www.thinkuknow.co.uk/)
- CEOPS and its role in the Virtual Global Taskforce (www.ceop.police.uk)
- Kidsmart, advice re privacy settings, etc. (www.kidsmart.org.uk)
- Childline has a section re online safety (www.childline.org.uk)

Internet Safety Tips

- Do not alter someone else's Facebook pages ("frappe"), which can have far-reaching, perhaps legal, implications, and do not make fake pages ("hate sites").
- Do not upload photos or comments that you would not want parents or teachers to see. Ask for permission before uploading or forwarding anything which might cause offence or be seen as "cyber-bullying". Errors of judgment made online can have an impact in school.
- As soon as you text, key-in, or upload anything there will be a permanent record of your actions on the Internet – as CEOP say, "you cannot delete".
- Take care with what you advertise about yourself – strangers should not be able to work out where you live, go to school, etc., from your Profile.
- Set all your Privacy buttons to their maximum values. Check them regularly as website administrators often alter what users are able to control.
- Do not have the same password for all your accounts – use numbers and letters, and keep them secret.
- Up-to-date security software, including a Firewall, is essential to keep you and your computer safe.
- Do not trust anyone on the Internet unless you know them personally. People can be deliberately deceiving.
- Do not click on pop-ups – they can make your computer vulnerable to viruses. Switch on your pop-up blocker.
- Do not reply to requests for personal information, such as phone numbers, PINs, and account numbers. This is known as "phishing" for information.
- Always log out of websites on shared computers both in school and in all public places.
- Take particular care on sites which involve web-cams – only use them to chat to people you know off-line too.

- When shopping online, ensure that the payment site is encrypted – look for the padlock symbol in the address.

Safety Use of Personal Electronic Equipment

- The school offers guidance on the safe use of social networking sites and cyberbullying in PSHE lessons which covers blocking and removing contacts from 'friend lists'.
- The school's guidance is that pupils and staff should always think carefully before they post information online. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.
- The school's PSHE lessons include guidance on how pupils can identify the signs of a cyber-stalker and what they should do if they are worried about being harassed or stalked online.
- The school offers guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.
- The school gives guidance on how to keep safe at home by encrypting the home wireless network, not opening unknown attachments and reporting any illegal content.
- Similarly the school covers how a mobile phone filter can be activated and how to block nuisance callers.
- The school advises on the responsible use of Skype and Facetime. But it appreciates that free video calls can provide boarders, particularly overseas boarders, with an invaluable means of maintaining contact with their families and friends.

Considerate Use of Electronic Equipment

- Mobile phones, smart phones, iPods and other personal electronic devices should be switched off and stored securely during the school day. They may be used during lunch-times and in boarding houses after school.
- Staff may confiscate personal equipment that is being used during the school day contrary to the school rules and will pass them to the DHP to whom the pupil should go to discuss their return.
- Sanctions may be imposed on pupils who use their electronic equipment without consideration for others.

The school expects all pupils to adhere to this charter for the safe use of the Internet. Copies are given to all pupils and their parents, and the school may impose sanctions for the misuse, or attempted misuse of the internet, mobile phones and other electronic devices.

Guidance for Parents from CEOP

Clicking this button from any website lets you access excellent information and advice from CEOP. It also allows you to submit a report to the police, who always investigate each report fully.

Parents are asked by CEOP whether they can say YES to EACH of the following points:

- I have installed a web-safe browser on our family computer(s).
- I have asked my child to show me sites they use.
- I have talked to my child's mobile phone provider about filtering software.
- I have asked my child to set all their profile settings to PRIVATE and to add "Click CEOP" to their profile.
- My child has agreed to tell me if they are worried about something they have seen or read online.

Finally

You cannot delete what you put out on the web - your actions, what you say, what you show, will ALWAYS exist somewhere on the Internet. Stay safe.

APPENDIX 5:

MEETING DITIGAL AND TECHNOLOGY STANDARDS IN SCHOOLS AND COLLEGES (DfE) – Andrew Hall

			Yes/No	Comment
A		**You should identify and assign roles and responsibilities to manage your filtering and monitoring systems**		
	A1	Have governors or proprietors identified and assigned a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met?		
	A2	Have governors or proprietors identified and assigned the roles and responsibilities of staff and third parties, for example, external service providers?		
	A3	Does the Senior Leadership Team understand that they are responsible for: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports		
	A4	Has the SLT ensured that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns		
	A5	Are arrangements in place for governors or proprietors, SLT, DSL and IT service providers to work closely together?		
	A6	Does the DSL should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems?		
	A7	Does the IT service provider have technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems		
	A8	Has the IT service provider worked with the senior leadership team and DSL to: • procure systems • identify risk • carry out reviews • carry out checks		
B		**You should review your filtering and monitoring provision at least annually**		
		Go to Review Questions		
	B1	Have governing bodies and proprietors ensured that filtering and monitoring provision is reviewed at least annually, to to identify the current provision, any gaps, and the specific needs of your pupils and staff?		
	B2	Are reviews conducted by SLT, DSL, the IT service provider and involve the responsible governor?		

	B3	Are the results of the online safety review recorded for reference and made available to those entitled to inspect that information?		
	B4	Does the review cover all required elements (as a minimum)?		
	B5	Have reviews informed:		
		• related safeguarding or technology policies and procedures		
		• roles and responsibilities		
		• training of staff		
		• curriculum and learning opportunities		
		• procurement decisions		
		• how often and what is checked		
		• monitoring strategies		
	B6	Does the review ensure that checks of the system have been carried out?		
		Go to Checks on filtering		
C		Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning		
		Technical requirements to meet the standard		
		Go here to see self-certified provider statements		
	C1	Is your filtering provider • a member of Internet Watch Foundation (IWF) • signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) • blocking access to illegal content including child sexual abuse material (CSAM)		
	C2	Is the school's filtering operational and applied to all: • users, including guest accounts • school owned devices • devices using the school broadband connection		
	C3	Does the filtering system: • filter all internet feeds, including any backup connections • be age and ability appropriate for the users, and be suitable for educational settings • handle multilingual web content, images, common misspellings and abbreviations • identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them • provide alerts when any web content has been blocked		
	C4	Has the provider confirmed that filtering is being applied to mobile and app content?		
	C5	Has a technical monitoring system been applied to devices using mobile or app content?		
	C6	Does the filtering system identify: • device name or ID, IP address, and where possible, the individual • the time and date of attempted access • the search term or content being blocked		
	C7	Are there any additional levels of protection for users on top of the filtering service, for example, SafeSearch or a child-friendly search engine?		

	C8	Are staff aware that they should make a report when: • they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs • there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material		
	C9	Does the school meet the Broadband Internet Standards?		
	C10	Does the school meet the Cyber Security Standards?		
		Two important elements of the Cyber Security Standards are that all staff who can access the IT Network have Basic CyberSecurity Awareness Training annually; and that at least one governor access this training.		
		Cyber Security Training from the National Cyber Security Centre can be found here as a PPT slide deck and a self-learn video		
	C11	Have all staff who use the school's IT Network had annual Basic Cyber Security Training?		
	C12	Has a least one governor attended a Basic Cyber Security training session?		
D		You should have effective monitoring strategies that meet the safeguarding needs of your school or college		
	D1	Does the monitoring system review user activity on school and college devices effectively? (For example, does it pick up incidents urgently, through alerts or observations, allowing prompt action to be taken; and is the response recorded?		
	D2	Has the governing body or proprietor supported the SLT to make sure effective device monitoring is in place which meets this standard and the risk profile of the school or college?		
	D3	Does the monitoring system ensure that incidents, whether of a malicious, technical, or safeguarding nature are picked up urgently?		
	D4	Is it clear to all staff how to deal with these incidents and who should lead on any actions?		
	D5	Does the DSL take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring?		
	D6	Has the DSL had training to ensure that their knowledge is current?		
	D7	Have IT staff had training to ensure that their knowledge is current?		
	D8	Does the school's monitoring technology apply to mobile devices or content used in apps?		
	D9	Are monitoring procedures reflected in the school's Acceptable Use Policy and integrated into relevant online safety, safeguarding and organisational policies, such as privacy notices?		
	D10	If the school has technical monitoring system, has a data protection impact assessment (DPIA) been completed?		
		A data protection impact assessment can be found here		

	D11	If the school has technical monitoring system, has a review the privacy notices of third party providers being undertaken?		
		Model privacy notices can be found here		

APPENDIX 6:

Filtering and Monitoring Checklist Register

In line with the DfE filtering and monitoring standards in schools and colleges, this checklist template has been developed as a basis to support schools and colleges in meeting the required standards. Whilst not intended to be exhaustive, this resource can serve as a summary record of checks highlighted within the standards.

Last updated:	Date:	Name/Position:

Roles and Responsibilities

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	
Senior Leadership Team Member	Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems	
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	

Reviewing your filtering and monitoring provision

Filtering System	
Filtering Provider and System	
Date Procured	
Date last reviewed	

Monitoring System	
Monitoring Provider and System	
Date Procured	
Date last reviewed	

Review Team [should be conducted by members of the senior leadership team, the Designated Safeguarding Lead (DSL), and the IT service provider and involve the responsible governor]	
Review Date	
Previous Review Date	
Link to last review	

Review Checklist	
the risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)	
what your filtering system currently blocks or allows and why	
any outside safeguarding influences, such as county lines	
any relevant safeguarding reports	
the digital resilience of your pupils	
teaching requirements, for example, your RHSE and PSHE curriculum	
the specific use of your chosen technologies, including Bring Your Own Device (BYOD)	
what related safeguarding or technology policies you have in place	
what checks are currently taking place and how resulting actions are handled	

all staff know how to report and record concerns	
filtering and monitoring systems work on new devices and services before release to staff / pupils	
blocklists are reviewed and they can be modified in line with changes to safeguarding risks	

Recommendations / Mitigating Actions

Data Protection Impact Assessment

Schools and colleges that have a technical monitoring system will need to conduct their own Data Protection Impact Assessment (DPIA) and review the privacy notices of third party providers

Link to DPIA	
Conducted by	
Date conducted	

Regular Reports

Type of Report	Filtering / Monitoring
Producer of report	
Recipient of report	
Frequency of report	

Monitoring data is received in a format that your staff can understand	
Users are identifiable to the school / college, so concerns can be traced back to an individual, including guest accounts	

System Checks

Filtering System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result

Confirm your filtering provider is:	
• a member of Internet Watch Foundation (IWF)	
• signed up to Counter Terrorism Internet Referral Unit list (CTIRU)	
• blocking access to illegal content including Child Sexual Abuse Material (CSAM)	

Monitoring System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result
