Cothill Policy Documents

ISSR 11 E-Safety Policy

NMS for Boarding: 4.1, 6.1, 6.2, 6.3, 14.4, 15.10

Date: September 2026
Next review: September 2027

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the community at Cothill with respect to the use of ICT.
- Safeguard and protect the children and Staff of Cothill.
- Assist School Staff working with children to work safely and responsibly with the internet and other communication technologies.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse.
- Ensure that all members of the School community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The E–Safety Policy is the responsibility of Adam Pearson (DSL) working alongside Andy Buck, Head of Group ICT, and Christopher Page, trained DSL and member of the Safeguarding Team. The E–Safety Policy and its implementation will be reviewed annually.

Roles and Responsibilities

This outlines the E-Safety roles and responsibilities of individuals and groups within Cothill School:

DSL, Headteacher & Head of Group ICT
The DSL has overall responsibility for E-Safety within the school and works with the Head & Head of Group ICT to ensure the School uses an approved, filtered internet Service (*Sophos*), which complies with current statutory requirements (EIS)
• The DSL, Headteacher & Head of Group ICT will be aware of procedures to be followed in the event of a serious E-Safety incident.
• The DSL, Headteacher & Head of Group ICT will ensure that there is a system in place to monitor and support Staff who carry out internal E-Safety procedures (e.g. network manager)

Head of ICT (Monitoring - CJP & Systems - JMP)

• Takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the School E-Safety policies / documents
• Promotes an awareness and commitment to E-Safeguarding throughout the School community
• Ensures that an E-Safety incident log is kept up to date
• Facilitates training and advice for all Staff
• Is regularly updated in E-Safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:

sharing of personal data, including Sexting
access to illegal / inappropriate materials
inappropriate online contact with adults / strangers
potential or actual incidents of grooming
cyberbullying and use of social media

• Oversees the delivery of the E-Safety element of the computing curriculum
• Liaises, when necessary with the DSL
• Ensures that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date)
• Ensures the security of the School ICT system
• Ensures that access controls / encryption exist to protect personal and sensitive information held on School-owned devices
• Ensures the School's policy on internet use is applied and updated on a regular basis
• Keeps up to date with the School's E-Safety policy and technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
• Ensures appropriate backup procedures exist so that systems can be recovered in the event of a disaster.

Teachers

• To embed E-Safety issues in all aspects of the curriculum and other School activities
• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended School activities if relevant)
• To ensure that pupils are aware of research skills relating to electronic content

All Staff

• To read, understand and help promote the School's E-Safety policies and guidance
• To read, understand, and adhere to the ICT Acceptable Use Policy (see Appendix)
• To be aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices
• To report any suspected misuse or problem to the E-Safety coordinator
• To maintain an awareness of current E-Safety issues and guidance e.g. through CPD
• To model safe, responsible and professional behaviours in their own use of technology
• To ensure that any digital communications with pupils should be on a professional level and only through School based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

All Pupils

• To read, understand, sign and adhere to the pupils' Responsible Use Policy (*See Appendix*).
• To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regs.
• To understand the importance of reporting abuse, misuse or access to inappropriate materials
• To know what action to take if they or someone they know feels worried or vulnerable when online.
• To know and understand School policy on the taking / use of images and on cyberbullying.
• To understand the importance of adopting good E-Safety practice when using digital technologies out of School and realise that the E-Safety Policy covers actions out of School, if related to their membership of the School
• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in School and at home
• To help the school in the creation/review of E-Safety policies

Parents/carers
• To support the School in promoting E-Safety
• To consult with the School if they have any concerns about their children's use of technology

Teaching and learning

Why is Internet use important?

Internet use is part of the statutory curriculum and is a necessary tool for learning.
The internet is a part of everyday life for education, business and social interaction.
Pupils use the internet outside school and need to learn how to evaluate internet information and to take care of their own safety and security.
The purpose of internet use in School is to raise educational standards, to promote pupil achievement, to support the professional work of Staff and to enhance the School's management functions.
Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

Benefits of using the internet in education include:

- access to worldwide educational resources including museums and art galleries
- educational and cultural exchanges between pupils worldwide
- access to experts in many fields for pupils and Staff
- professional development for Staff through access to national developments, educational materials and effective curriculum practice
- collaboration across networks of schools, support services and professional associations
- improved access to technical support including remote management of networks and system updates

- access to learning wherever and whenever convenient

How can Internet use enhance learning?

The School's internet access will be designed to enhance and extend education.
Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
Access levels to the internet will be reviewed to reflect curriculum requirements and the age and ability of pupils.
Staff should guide pupils to online activities that will support planned learning outcomes.
Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
Pupils will be taught to acknowledge the source of information used and to respect copyright.

How will pupils learn how to evaluate Internet content?

Pupils will be taught to be critically aware of the materials they read.
Pupils will use age-appropriate tools to research internet content.
The evaluation of online materials is a part of teaching and learning in every subject.

How will information systems security be maintained?

The security of the School information systems and users will be reviewed regularly.
Virus protection will be updated regularly.
Unapproved software will not be allowed in work areas or attached to email.
All files held on the School's network are accessible by CJP
The Head of Group ICT will review system capacity regularly.
The use of user logins and passwords to access the School network will be enforced.

How will email be managed?

Pupils may only use approved email accounts for School purposes.
Pupils must immediately tell CJP if they receive an offensive email.
Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
Staff will only use official School provided email accounts to communicate with pupils and parents/carers
Access in School to external personal email accounts may be blocked.

How will published content be managed?

The contact details on the website should be the School address, email and telephone number. Staff or pupils' personal information will not be published
The Headmaster will take overall editorial responsibility for online content published by the School and will ensure that content published is accurate and appropriate.

Can pupils' images or work be published?

Images or videos that include pupils will be selected carefully before publication on the School website. Content will never be hosted on external servers except for photos taken by touchline parents at matches which will appear on Google Photos, and videos from the School website which may appear on the (unlisted) YouTube Channel for Cothill.
Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
Websites created by pupils may occasionally be shared with parents, as permitted by teachers in ICT Dept.

How will social networking, social media and personal publishing be managed?

The School will control access to social media and social networking sites. At the time of writing, access to all social networking sites is prohibited on the School network for all pupils. An exception is made for GAP students who are permitted access to Facebook & Snapchat on their mobile phones.
Pupils will be advised not to give out personal details of any kind which may identify them and/or their location.
Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. • Staff are well aware of the possibilities and dangers of grooming taking place online and pupils will be advised accordingly.
All members of the School community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
Concerns regarding students' use of social networking, social media and personal publishing sites (out of school) may be raised with their parents/carers, particularly when concerning students' underage use of sites.
All pupils receive e-safety lessons across Years 3, 4, 5, 6, 7 and 8..

How will filtering be managed?

The School's broadband access will include filtering appropriate to the age and maturity of pupils. In addition, the software called Securly is used to filter all online content accessed by pupils at school.
If Staff or pupils discover unsuitable sites, the URL will be blocked on Securly and then should be reported to CJP who will then take the appropriate action

How is filtering managed outside of term time?

All school-managed devices and networks continue to be protected by filtering systems at all times. These systems are designed to block access to inappropriate, harmful or illegal content and remain fully operational whether pupils are in school or at home. Outside of normal school hours, alerts are not reviewed in real time. Instead, they are recorded and reviewed by safeguarding staff when the school reopens or when staff return to duty.

When school is not in session, immediate safeguarding support is not provided through school systems. If a pupil is using a school-managed device during these times, parents and carers play an important role in supervising and supporting their child's online activity. This includes:

- Discussing safe online behaviour
- Monitoring device use where appropriate
- Ensuring age-appropriate access to apps, games and websites

Where appropriate, parents and carers may also take a more active role in monitoring their child's device when it is used outside of school hours. Please contact the school IT team for further information on how this can be enabled.

How are emerging technologies managed?

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in School is allowed.
Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the School Acceptable Use Policy.

How should personal data be protected?

Personal data will be recorded, processed, transferred & made available according to the Data Protection Act 2018.

Policy Decisions

How will Internet access be authorised?

The School will maintain a current record of all Staff and pupils who are granted access to the School's electronic communications.
Staff are requested to read the School Acceptable Use Policy (*Cothill Policies Book*) before using any School ICT resources (Appendix)
As a rule, visitors and parents will not be given access to the School's wifi network, although exceptions may be made by the SLT in special circumstances.
Pupils will be provided with supervised internet access appropriate to their age and ability.
When considering access for vulnerable members of the School community (such as with children with SEN) the School will make decisions based on the specific needs and understanding of the pupil(s).
Pupils can only access the internet at school on Chromebooks and Chromeboxes.
Pupils will not be allowed online at School without being supervised.

How will risks be assessed?

The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of the internet, it is not possible to guarantee that access to unsuitable material will never occur via a School computer. The School cannot accept liability for the material accessed, or any consequences resulting from internet use.

The School will audit ICT use to establish if the E–Safety policy is adequate and that the implementation of the E–Safety policy is appropriate. Methods to identify, assess and minimise risks will be reviewed regularly.
The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Serious Crime Act 2015

How will the School respond to any incidents of concern?

All members of the School community will be informed about the procedure for reporting E-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
CJP will record all reported incidents and actions taken in the School E-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
The Designated Safeguarding Lead will be informed of any E-Safety incidents involving Child Protection concerns, who will deal with them appropriately.
The School will manage E-Safety incidents in accordance with the School Discipline Policy where appropriate.
The School will inform parents/carers of any incidents of concerns as and when required.
After any investigation, the School will debrief, identify lessons learnt and implement any changes required.
Where there is cause for concern or fear that illegal activity has taken place or is taking place then the School will contact the E-Safety officer and report to the Police.

How will E–Safety complaints be handled?

Any complaint about Staff misuse will be referred to the Headmaster.
All E–Safety complaints and incidents will be recorded by the School, including any actions taken.
All members of the School community will need to be aware of the importance of confidentiality and the need to follow the official School procedures for reporting concerns.
Any issues (including sanctions) will be dealt with according to the School's disciplinary, behaviour and child protection procedures. (See the *Behaviour Policy*).
All members of the School community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the School community.

How will Cyberbullying be managed?

See ISSR 7 & 8 Safeguarding Policy

Cyberbullying (along with all other forms of bullying) of any member of the School community will not be tolerated. Full details are set out in the School's policy on Countering Bullying and Discipline.
All incidents of cyberbullying reported to the school will be recorded.
Pupils, Staff and parents/carers will be advised to keep a record of the bullying as evidence.
The School will take steps to identify the bully, where possible. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider, if necessary.

Internet access may be suspended at School for the user for a period of time. Other sanctions may also be used in accordance with the School's Countering Bullying Policy, Discipline Policy or Acceptable Use Policy.
Parents/carers of pupils will be informed.
The Police will be contacted if a criminal offence is suspected.

How will mobile phones and personal devices be managed?

See the Specific Items Policy.
School Staff may confiscate a phone or device if they see them being used by students.
Electronic devices of all kinds that are brought into School are the responsibility of the user. The School accepts no responsibility for the loss, theft or damage of such items. Nor will the School accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Staff Use of Personal Devices

Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Mobile phones or devices should not be used during teaching periods except in emergency circumstances.

If members of Staff have an educational reason to allow pupils to use mobile phones or personal devices as part of an educational activity, then it will only take place when approved by the Headmaster.

Staff are only allowed to use personal equipment (e.g. their own mobile phones) to take photographs of pupils if taking the photos directly onto the school's Google platform. Refer to the Photography of Pupils Policy.

Communication Policy

How will the policy be introduced to pupils?

All users will be informed that network and internet use will be monitored.
Teachers of ICT provide regular reminders to pupils to ensure that they are aware of the importance of safe use of the internet. An E-Safety presentation is given by an outside agency to Years 7 and 8.
Pupil instruction regarding responsible and safe use will precede internet access.
Safe and responsible use of the internet and technology will be reinforced across the curriculum and subject areas.
Particular attention to E-Safety education will be given where pupils are considered to be vulnerable.

JMP/CJP - September 2026

Appendix: E-Safety References

Guidance is available from the Department of Education here. This is Teaching online safety in school (June 2019).

KCSiE Annex D has a section on online safety. Find the document here.

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

UK Safer Internet Centre : https://saferinternet.org.uk/

ICT Acceptable Use Policy for staff

As a professional organisation with responsibility for children's safeguarding it is important that all Staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites.
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of Staff. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security

information.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely.
- Professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), will not be shared with others outside School. I will protect the devices in my care from unapproved access or theft.
- I will respect copyright and intellectual property rights.
- I will report all incidents of concern regarding children's online safety to the DSL, CJP or Head.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to a Head of ICT as soon as possible.
- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number.
- My use of ICT and information systems will always be compatible with my professional role, whether using School or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the School Acceptable Use Policy and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the School into disrepute.
- I will promote E-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practice online either in School or off site, then I will raise them with the DSL or Headmaster.
- I understand that my use of the School's information systems, internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including internet access and the interception of emails in order to monitor compliance with this Acceptable Use Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

ICT Acceptable Use Policy for Cothill pupils

All pupils must complete this form before they can use the computer room. These rules will keep everyone safe and help us to be fair to others. Your email address will be recorded when you submit this form.

PTO for 1:1 Policy guidelines
1:1 Chromebooks Scheme
All pupils agree to comply with all of the following rules:

Do you accept the following points about the use of your chromebook?

I learn online – I use the school's internet and Chromebooks for schoolwork, homework and other activities to learn and have fun. I accept that school internet and devices are monitored.
I ask permission – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to. I will not try and get around restrictions, such as trying to access YouTube.
I am a friend – I won't share anything that I know another person wouldn't want to be shared, or which might upset them. I will be kind and respectful when interacting with others online. If I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
I am a secure – I keep my passwords and private information (such as my address) to myself and reset them if anyone finds them out. Friends don't share passwords! I will also never try and access someone else's account.
I am a careful clicker – I don't click on unexpected links or popups. If I am not sure I ask an adult.
I ask for help – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
I keep my body to myself online – I never show what's under my clothes in front of a camera.
I tell my parents what I do online – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
I am private online – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends.
I am careful – I know anything I do can be shared and might stay part of my digital footprint forever.
I am a rule-follower online – I know that apps, sites and games have rules on how to

behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour. I will not steal or illegally download videos, music, etc.

I respect my school - I am entrusted to use technology in a respectful way. I will not try and 'get around' filtering, and will only use my Cothill google account at school. If I do not use it in this way, I accept that I may be restricted from using technology.

* Indicates required question

Email *

☐ Record **cpage@cothill.org.uk** as the email to be included with my response

I agree and my **name** is *

Your answer

Which class are you in? *

Choose

Thank you for completing the form. We expect you to behave when using your Chromebook as view it as an educational tool, not a toy.

Key Points

- Each pupil can only use their own device - no sharing allowed except when borrowing a spare Chromebook.
- Year 3 and 4 Chromebooks are provided by the school.
- In Years 3-7, devices are to only be brought to lessons when requested by the class teacher. Year 8 may carry their device with them during the day.
- Devices must be stored in charging cabinets overnight. Years 3-7 store these in the ICT room, and 8 in their classrooms.
- The Golden Rule: Chromebooks are never to be used unsupervised by pupils.
- All Chromebooks are managed by the IT department. Thus, online access can be switched on and off.
- Beyond exceptional circumstances, which will be communicated by the ICT department, Chromebooks are accessible for lessons when approved by the lesson teacher, during form time when approved by the form tutor, for relevant CAPs (such as computing club or the school paper), and when required for prep.
- ‘Out of hours’, no online access is available to pupils.
- Online access will be provided during Free Time & Sundays at the discretion of the IT department and on duty staff.
- In Free Time, pupils may only use their Chromebooks in a supervised space, such as the ICT room or a teacher’s classroom.
- Pupils can borrow school headphones, or can bring in their own without batteries/bluetooth.