Cothill House Policy Documents

ISSR 11 Health & Safety

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

Date: January 2019
Next review: spring 2019

Health and Safety Policy - General Statement of Intent (see Trust Intranet):

THE COTHILL TRUST

Health and Safety Policy: our General Statement of Intent 2018

So far as is reasonably practicable, with the help of its employees and taking regard to government guidance on Health & Safety Responsibility, The Cothill Trust will:-

- provide adequate control of the health and safety hazards and risks arising from Trust activities
- consider our common law *in loco parentis* duties to all pupils in our care
- consider under Health and Safety at Work Act (1974) S3, our statutory duty of care to pupils and other non-employees
- consult with our employees (and their representatives) on matters affecting their health, safety and welfare
- ensure all employees are competent to do their tasks
- provide information, instruction, training and supervision for employees
- provide and maintain safe housing (where provided), plant, equipment and processes
- promote safe handling and safe use of all hazardous substances
- prevent accidents and ill health by promoting safe healthy working conditions
- take full advantage of technical expertise within the Trust to monitor and regulate the working environment
- be aware of the philosophy contained within HSE documentation
- review and revise this policy as necessary at regular intervals

Tom Beardmore-Gray

Tom Beardmore Gray – CEO August 2018

If you have any questions or concerns about Health and Safety, please contact Chris Gillham in the Trust Office
Telephone: 01865 390720 ~ Email: cgillham@cothilltrust.org

The Cothill Trust, 7 Cothill, Abingdon, Oxon OX13 6JN
01865 390720 www.cothilltrust.org

Chairman: Dr Ralph Townsend - Chief Executive: Tom Beardmore-Gray MA FCA
Registered Company No. 961616 Registered Charity No. 309639

E-Safety

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the community at Cothill House with respect to the use of ICT.
- Safeguard and protect the children and Staff of Cothill House.
- 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 students.

The E–Safety Policy is the responsibility of John Carver, Head of ICT. 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 House School:

Headteacher

• To take overall responsibility for E-safety provision
• To ensure the School uses an approved, filtered internet Service (*Barracuda*), which complies with current statutory requirements (EIS)
• To be aware of procedures to be followed in the event of a serious E-Safety incident.
• To 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

• 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 Boys' 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 the Head of ICT.
The Head of 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 the Head of ICT if they receive 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 House.
Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

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 Staff & GAP students - bar some who live on site - and pupils.
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.
In Years 7 & 8, pupils receive training in E-Safety, as do Juniors in Years 4 & 5.
How will filtering be managed?
The School's broadband access will include filtering appropriate to the age and maturity of pupils.
If Staff or pupils discover unsuitable sites, the URL should be reported to the School E-Safety Coordinator who will then take the appropriate action

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 1998.

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 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 Head of ICT in special circumstance
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 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 Computer Misuse Act 1990

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).
The Head of ICT 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.
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 to the School's Countering Bullying Policy, Discipline Policy or Acceptable Use Policy.
Parent/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 in to 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 children to use mobile phones or personal device as part of an educational activity, then it will only take place when approved by the Headmaster.
Staff will not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will use Cothill equipment for this purpose. See the Head of ICT for school cameras.

Communication Policy

How will the policy be introduced to pupils?

All users will be informed that network and internet use will be monitored.
The Head of ICT provides 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.

Karl Hopwood of *ChildNet International* speaks annually to Years 6, 7 & 8 regarding E-Safety. On the same day, the parental body is invited to attend an address by Mr. Hopwood.

Appendix: E-Safety References

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

Childline: www.childline.org.uk

Childnet: www.childnet.com

Children's Safeguards Team: www.kenttrustweb.org.uk?safeguards

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

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

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

Kidsmart: www.kidsmart.org.uk

Schools E–Safety Blog: www.kenttrustweb.org.uk?esafetyblog

Teach Today: http://en.teachtoday.eu

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

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

ICT Acceptable Use Policy

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 Head of ICT or Headmaster
- 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 the 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 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.

Cothill House School

Boys' Responsible Internet Use

- We use the School computers and internet connection for learning. These rules help us to be fair to others and keep everyone safe.
- I will only use my own Google login and password.
- I will not access or delete any one else's work.
- I understand that I must not bring software, disks, USB sticks into School without permission.
- The emails that I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- I will not use Internet Chat Rooms.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher (AJRC) immediately.
- I understand that if I deliberately break these rules, I will be punished and banned from using the computer room

Access to Pupils, Contractors & Security

Introduction
Contractors visiting Cothill have to sign in & out at the Domestic Bursary or School office. Passes on lanyards are issued. Outside contractors, workmen, etc are not permitted unsupervised access to the boys. Other visitors (prospective parents, etc) are booked via the School Secretary and will report to the Office in the first instance. No visitors are permitted unsupervised access to the boys and will be accompanied by Staff as necessary. This includes visiting speakers & prospective staff on interview.

CCTV is installed to monitor traffic into the main car park, the Bursary and Bowlers' entrances.
At Chandlings, CCTV covers the main gates, driveways and back of the school buildings.

Buildings
All external doors are locked at night, once the boys have gone upstairs to their dormitories.

Cothill Main Building:	8.15 - 8.45pm
Bowlers:	8 - 8.30pm
Chandlings:	c. 9.30pm

Gates & keycoded entry doors remain locked throughout most of the day. In order to control access to the boys - especially at night - and to satisfy inspection criteria, codes for doors to the Main Building at Cothill are released on a need to know basis. (Code last changed summer 2017.)

Parents may accompany children to the dormitories at the beginning of term or at the end of an Exeat or Half Term; moreover, visitors on tours will be taken on conducted tours around dormitories. Otherwise, visitors are not allowed into the dormitory area of the school when the boys are present. The Head Matron will be informed of any exceptions and will ensure that no unsupervised access is permitted.

Neither parents nor visitors are permitted access to changing areas, showers or lavatories when boys are present.

In the event of a situation where access to boys is required by a person independent of the School Staff group, a member of Staff will ensure that permission has been sought for this, and that appropriate consideration of the risks involved has been considered (e.g. showing parents around the School, visiting the doctor etc.)

Vehicular Entry
There is keycoded entry for vehicular gates.

The main car park gates: closed most of the time, access being via a coded keyring device. Visitors in cars can gain access via an intercom which contacts first, the Bursary, failing that, the Office, and failing both of these options, the Headmaster's mobile phone.

Cothill Main Car Park Gate Regular Opening Times:

Weekdays	Open 6.45am – 9.30am (to allow Staff to enter) Open 7.15pm – 7.45pm (for Chandlings boarders' evening transport)
Match Days (Wed & Sat)	Open 1pm -5pm
Saturdays	Open 6.45am – 9.30am
Sundays	Open 6.50am – 12 noon (allowing parents to pick up their sons) Open 5.30pm -9pm (allowing parents to return their sons)
Friday Exeats & Half Term	Open 6.50am – 9.30am *then* 12.30pm -3.30pm
Sun & Mon Exeat return	Open 4.30pm -9pm
Thursday start of term & morning returns	*Open* 6.50am – 12.30pm

The gates open automatically when a car approaches them from inside the car park.

The Bursary gates into the Yard: closed most of the time with access only via coded keypad. These gates are opened when parents drop off or pick up their children.

The Headmaster's entrance gates: open 7am - 7pm. At other times, access is via a coded keyring device.

Chandlings gate: open 7am - 9.30pm. At other times, access is via a coded keyring device.