OLD BUCKENHAM HALL

A leading co-educational preparatory school for children aged 2-13 years

e-Safety Policy

OBHP09

Policy owner: IT Network Manager
Date of issue: August 2025
Policy revised: August 2025
Next review due: August 2026

Introduction

Please note: this Policy must be read in conjunction with Policy OBHP08 (AUP for Staff.)

Technologies are constantly evolving and therefore any policy needs to be as dynamic as possible and under constant review. The school needs to be sufficiently flexible to manage new and emerging technologies, as they may have important educational and social benefits. The policy aims to balance the use of existing and emerging technologies with the necessity of providing safeguards for pupils and employees against risks and unacceptable material and activities.

The Internet is an essential element for education, business and social interaction. Although our location is in a 'difficult' area for access, the school provides the best quality Internet access it can, in order to enhance the learning experience. Currently, our access is via a dedicated 1Gbit fibre link (leased line.)

The school provides filtered Internet access for pupils together with a school Microsoft 365 email account and file storage, both locally, on the school's network servers, and in the Cloud, via Microsoft 365's OneDrive online storage. A 'Moodle' Virtual Learning Environment is also available, allowing pupils to have easy access to a variety of online resources and providing them with a convenient way of submitting work to their teachers and having it marked online where appropriate. We have a duty to educate pupils to use these technologies safely and with due regard for others.

Although children may be trusted by their parents with regard to private Internet use, schools have a duty to safeguard them and to educate them to use online material safely and responsibly. Parents need to be reassured that their child is not able to access material deemed unsuitable and/or in contravention of the school's Acceptable Use Agreement. Additionally, many parents appreciate guidance from schools regarding their children's use of online technologies and platforms.

Keeping Children Safe in Education 2025

This policy takes into account elements of KCSIE 2025 relevant to online safety.

Online safety is clearly viewed as part of a school's statutory safeguarding responsibilities. Indeed, online safety is now very much interwoven with safeguarding in general. A designated School Governor - Charlotte Marten- has a particular responsibility for Safeguarding and E-Safety. The Designated Safeguarding Lead has overall responsibility for online safety and is supported by an e-Safety lead person and Deputy DSLs. The e-Safety Lead is currently Mr Andrew Swiney, supported by John Sibley, IT Network Manager.

These statements in KCSIE 2025 are important:

> *The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:*
>
> - content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
> - contact: being subjected to harmful online interaction with other users; for example: peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
> - conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying,
> - commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

It also refers to the provision of appropriate filtering and monitoring systems - whilst acknowledging that 'over-blocking' can lead to staff and pupil frustration - and a 'whole school' approach to online safety. Filtering must take into account the school's Prevent duty and protect children from terrorist and extremist

material. Staff training in online safety should be regarded as an integral part of the school's approach to Safeguarding. All staff undertake annual cyber security training.

Online safety training | NSPCC Learning

A school should also have a clear policy on the use of mobile devices; many children now have unlimited and unrestricted access to the Internet through mobile networks (3G/4G/5G.) Whilst at OBH the use of such mobile devices is strictly controlled, it is recognised that children use these at home and parents are warned about the inherent risks by the School, in e-Safety talks from visiting speakers and in weekly updates in the OBH Times .

This e-Safety Policy applies to the whole school, including EYFS and Pre-Prep department.

The school will:

- Provide appropriate training in e-Safety for staff and support any staff and pupils having online safety issues.
- Provide educational material and support for parents.
- Provide policies for e-safety and acceptable use that are clear and easily understood.
- Make clear to pupils and staff how they can seek help if they have any concerns.
- Make clear what the risks are of using the Internet irresponsibly.
- Encourage pupils and staff to be discerning regarding material found on the Internet.
- Make pupils and staff aware of the Acceptable Use Policies and the sanctions in place to enforce them.

Network procedures and practices

The school provides pupils and staff with Internet access and access to the school's own network through both wired and wireless connections across the site. Pupils and staff have an individual username and password with the means to create and save files on the school network and in the Cloud, via Microsoft's OneDrive online storage platform. All pupils and staff have a private area, both on the network and in the Cloud, which can only be accessed using their particular account credentials.

The school's Internet access is provided by Wavenet via a leased line fibre link. Both Staff and Pupil logons are filtered for Internet access by both LightSpeed and a Cisco Meraki MX firewall appliance. LightSpeed allows different levels of access according to year group. School PCs accessed by pupils have NetSupport, Lightspeed and Sophos AV (antivirus) agents installed on them - details are towards the end of this section. Cisco, Sophos, NetSupport and Lightspeed are all members of the Internet Watch Foundation.

The IT Network Manager together with the Head of Computer Science (the current e-Safety Lead) regularly monitors the correct operation of the filtering systems. General network traffic and the performance and security of the network are constantly monitored using the Cisco Meraki MX firewall, Sophos Central AV system, NetSupport and other software.

The computer network is owned by the school and may be used by pupils to advance and extend their knowledge and understanding. The school will exercise its right to monitor the use of computer systems, including the monitoring of Internet use and the email system, and the deletion of inappropriate materials at all times. System logs may also be inspected at the request of the SMT, any DSL or the Head of Computer Science in the event of a concern.

In circumstances where the school believes unauthorised use of the computer system is, or may be taking place, or the system is, or may be, being used for unlawful purposes, the school reserves the right to inform appropriate authorities and provide documentary evidence.

Pupils should be aware that their files, e-mails and other forms of electronic information storage and communication (including any external storage media which pupils bring into the school) may be scrutinised for the purposes of safeguarding or promoting a child's welfare. This would normally be authorised by the Headmaster, Deputy Head or SMT.

Although all staff and pupils are expected to use ICT responsibly and receive specific education to define and encourage responsible use, the school recognises that it has a responsibility to counter any attempts at irresponsible behaviour which may still arise. The school's ICT system is monitored and managed in a number of ways designed to inhibit abuses, as described in the following paragraphs:

- Web Filtering – the school subscribes to reputable services (LightSpeed / Cisco Meraki). Some website categories are banned permanently, some are restricted to adults only. The filters are updated continuously and are regularly checked for correct operation. All PCs/laptops connected to the school's network domain are filtered by LightSpeed and have their 'Smart Agent' software installed. Some categories of sites are blocked for some age groups and not others - for example, older pupils are permitted restricted use of YouTube. Other devices connected to the school's network are filtered by the Cisco Meraki MX firewall appliance. 'Safe search' for Google and other search engines is enforced for pupils/staff throughout the site.
- Mail Filtering - We use Microsoft 365 for email, providing an encrypted connection between the device and Microsoft's servers. Incoming and outgoing Junk (spam) emails, and also any emails containing malware, are filtered. Appropriate staff can send sensitive data (e.g. safeguarding, medical) by secure email (the IT Network Manager can provide further details.)
- Logs - all pupil user data is recorded on our NetSupport system. All website requests, windows opened and applications used are logged and users are taught this. NetSupport also has a keyword system for categories such as sites with sexual content, grooming, bullying and radicalisation content. All pupil activity on the Internet is logged by Lightspeed, including details of searches, sites accessed and blocked, etc.
- Social Networking sites – access to these is blocked for pupils.

Use of mobile devices on the network

Pupil use of devices such as e-readers, tablets, mobile phones and smartwatches is strictly controlled. Pupils are not allowed mobile devices, with the following exceptions:

- International pupils who are full boarders hand their devices in on return to school. With permission from boarding staff, they are issued them under supervision in order to contact their families.
- Basic Kindles are allowed for reading. For boarders, these are handed to boarding staff at lights out and returned the following day. If temporary network access is required to download a new book, the IT Network Manager or Head of Computer Science will supervise this.
- Pupils may only have an iPad or laptop at school if this has been permitted by the SENCO, Mrs Gemma Gillott. Devices are returned to her room at the end of the school day. There is at present a set of iPads in the ICT Room that may be booked out by staff. They must be connected to the network using a dedicated Wi-Fi SSID (OBH Pupil Devices) which is filtered and available only during school hours.

Areas of risk

Whilst access to the Internet is filtered as described in the previous sections, it is acknowledged that there are still areas of risk, as follows:

Content

- exposure to inappropriate content
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- Online peer-on-peer abuse and cyber-bullying in all forms
- grooming
- identity theft and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online)
- sexting (sending and receiving of personally intimate images)
- copyright (little care or consideration for intellectual property and ownership, such as music and film)

Commerce

- Risks such as online gambling and inappropriate advertising
- Phishing (the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers)
- financial scams

The school seeks to minimise these risks through a combination e-Safety lessons, discussions, assemblies and workshops with visiting specialists. Children are made aware of the Acceptable Use Policy for the computers, which is displayed in the ICT Room and throughout the school. E-Safety is not regarded as the responsibility of ICT staff alone; Form Teachers are encouraged to discuss issues with their classes as part of the PSHE programme and Subject Teachers to remind classes of best practice whenever online resources are being used.

NetSupport School

This network management software contains keyword libraries which compare all text entries by children against databases for adult content, radicalisation, grooming, sexting, bullying, possible self-harming and eating disorders. If a suspect word is typed – it is logged along with a screenshot so that the ICT staff can monitor regularly on a contextual basis. Thus misuse of the computers – e.g. inappropriate searches – is almost certain to be noticed and investigated. In most cases though, the context provided by the screen shot will show that there was no intended misuse – e.g. the word 'bomb' typed by a pupil writing a story on WW2 being flagged under the radicalisation category.

The Prevent Strategy

We are very much aware of our responsibilities under the Prevent strategy. Any staff with concerns about a child should pass these on without delay to the Safeguarding DSL, Mrs Emma Easdale, or in her absence to the DSL Alternates –Graham Drury,

Our NetSupport software monitors, captures and logs words typed in by pupils who might show an interest in extreme violence or radicalisation. See the previous section for details.

Access to ICT Facilities

Pupils may access the ICT Room is from 0800 under supervision.

Evenings after supper: boarders are allowed in the ICT Room from 19.30hrs to email their parents and play educational games. Duty staff supervise.

This, in conjunction with the filtering in place, minimises the risk. Social networking sites are blocked for the children at school, as are webmail accounts such as Hotmail. Staff having concerns regarding sites which the children access must report these to the IT Network Manager.

At weekends, boarders can access the computers in the library under supervision.

Restrictions for pupils

- Pupils may only use the school email system. Webmail (e.g. Hotmail) is blocked.
- Chat rooms and social networking sites are blocked.
- Gambling and e-commerce sites are blocked.
- Other blocked categories include pornographic, hate and discrimination, violence, drugs, weapons, offensive and tasteless, newsgroups and forums, media streaming & downloading.

Expectations of pupils and parents beyond the school

When a pupil is at home, families bear responsibility for the guidance of their children. The school expects the use of ICT by its pupils, even when at home, to comply with the school's stated ethos. Material downloaded in the home, posted on an Internet site from a home computer, or transmitted to/from a mobile phone when a pupil is at home, can impact significantly upon the life of pupils at school. Thus we ask all parents/guardians to cooperate with the school in the education of their children in the use of ICT.

E-Safety Roles at OBH

Headmaster / DSL / SMT

- Assume overall responsibility for e-safety.
- Ensure that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant.
- Are aware of procedures to be followed in the event of a serious e-safety incident.

The Governor with responsibility for Safeguarding and e-Safety

- The Governor who oversees Safeguarding and e-Safety is Charlotte Marten
- Termly meetings of the Safeguarding Committee are held and minutes are kept of the meetings. The Committee comprises the Governor with responsibility for Safeguarding, the Headmaster, the DSL and the two Deputy DSLs, the E-Safety Lead and the IT Network Manager.
- A variety of matters including e-Safety training and education are discussed at these meetings.
- The e-Safety/Safeguarding Governor reports back to the full Governing Board on a termly basis. A short section on e-Safety is included in the termly Safeguarding report to the Governors.

E-Safety Lead / DSL / IT Network Manager

- Takes day-to-day responsibility for e-Safety issues and has a co-ordinating/leading role in establishing the school's e-Safety policy.
- Promotes an awareness and commitment to e-safeguarding throughout the school community.
- Liaises with PSHE teachers and ensures that e-Safety education is embedded across the curriculum.
- Liaises with the school's IT Network Manager.
- Reports to the Headmaster / SMT / DSL to discuss current issues, report and review any incidents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.
- Ensures that an e-safety incident log is kept up-to-date and is signed termly by the Governor with responsibility for Safeguarding.
- Organises specific e-Safety events, including assemblies and workshops with experts from outside the school. These events should include parents.
- Facilitates training and advice for all staff.

IT Network Manager (Mr John Sibley)

- To report any e-Safety-related issues that arise to the E-Safety Lead.
- To ensure that users may only access the school's networks using the relevant username and password, and to encourage the use of strong passwords which may be reinforced by the use of Multi-Factor Authentication (MFA) where appropriate.
- To ensure that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date.)

- To ensure the security of the school's ICT systems, liaising with system vendors and other support entities when necessary.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices and storage facilities.
- To ensure that the Lightspeed filter is maintained and working properly on a regular basis.
- Ensure that they keep up-to-date with the school's e-Safety policy and the relevant technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant.
- To ensure that the use of the school's network, remote access and email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Lead / SMT for investigation / action / sanction.
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

All Staff

- 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 fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- To read, understand and help promote the school's e-safety policies and guidance.
- To be aware of e-Safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- To be aware that child-on-child sexual violence / harassment can occur online, at home or at school.
- To report any suspected misuse or problem to the e-Safety Lead and the DSL via CPOMS.
- To maintain an awareness of current e-Safety issues and guidance e.g. through CPD.
- To set a safe, responsible and professional example 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. See also the Staff AUP.

Parents

- To support the school in promoting e-Safety .
- To read, understand and promote the school's Pupil Acceptable Use Agreement with their children.
- To consult with the school if they have any concerns about their children's use of technology.
- To attend, where possible, any workshops that have been organised by Old Buckenham Hall about any issues relating to e-Safety.

Pupils

- To read and understand the Acceptable Use Policy for pupils.
- 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 using online technology.
- To know and understand school policy on the taking / use of images and on cyber-bullying.
- To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their 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

Appendices

OLD BUCKENHAM HALL
A leading co-educational preparatory school for children aged 2-13 years

Agreement for safe and appropriate use of ICT facilities – September 2025

All pupils in the Upper School at OBH are asked to read the following document giving rules for responsible use of the ICT facilities. This document is discussed in Forms and Computer Science lessons to ensure that pupils understand why these rules are to be used.

Introduction

The school provides a variety of devices with Internet access to help you with your learning. There is also 'Office 365', which gives you email which you can use to contact your friends and family - and also cloud storage where you can store documents which you can work on at school or at home. All pupils are given email addresses at the start of the year.

So that everyone at OBH uses the computers safely and with due consideration for others, we need to have some rules which you must follow.

We have tried to keep these rules as simple as possible so that everyone can understand them.

Using the Computers

- **If I am worried about anything I find on the computers I will tell a member of staff.**
- I will only access the computer system using the username and password I have been given.
- I will not give my username and password to anyone else.
- I will use the computers sensibly and not interfere with any of the wiring or the settings of the computers. When I have finished I will leave the computer tidy for the next person.
- I will not attempt to access others' files or emails.
- I will not bring in CDs, DVDs or USB drives from outside school and try to use them on the school computers without permission from the IT Network Manager or the Head of Computer Science.
- I understand that the computers are provided primarily for work. Use of them for games during the working day is not allowed.

Using the Internet

- **If I see anything or receive any messages that concern me, I will tell a member of staff immediately because this will help protect other pupils and me.**
- I will not deliberately search for inappropriate material on the Internet.
- I understand that all my use of the computers is recorded and that the ICT staff may check my computer files and the sites that I visit.
- I will not give away any personal information to any sites on the Internet. If I am not sure about this, I will ask a member of staff.
- I will not download any files or applications without permission from Mr. Swiney, except images to be used in class or project work.

- I will not attempt to use any chat rooms or social networking sites.
- I will not copy or download work from the Internet and claim it as my own.

Using e-mail and Office 365

- **If I receive an email that I am worried about or that I find unpleasant, I will not delete the email but will tell Mr Leeson, my Form Teacher or Tutor as soon as possible.**
- I will only e-mail people I know. For my own safety I will not give any personal details such as my email address, home address or phone number to people or organisations that I do not know.
- I will not use the email system to send games or inappropriate material to other people.
- I will only use the Cloud Storage (OneDrive) for storing work-related material.
- I understand that use of my school email / Office 365 account from home or elsewhere is still subject to the terms of this Policy.

Remote Learning using MS Teams and other software provided by OBH

- I understand that whilst engaging in remote learning, the Acceptable Use Policy still applies. I will use the system responsibly with due consideration for others.

Personal Devices

- If permitted to use a device at school, I understand that this is only to assist in my classroom learning. It is not to be used for playing games. Emails must be sent via my school address and should only be work-related.
- If I am boarding, the device will be stored securely in agreed areas after prep. If I am not boarding, the device will be taken home. I will ask a member of staff if I need assistance charging my device.
- Use of my personal device at school is still subject to the Acceptable Use Policy. I will use the OBH Pupil Devices Wi-Fi SSID to connect to the Internet.
- I will not let anyone else use my device. I will ask a teacher if I need help using it in the classroom.

Deliberate Misuse

- I understand that deliberate misuse of any ICT device may result in action being taken.

Remember that these rules are for your own safety.

If you are concerned about anything, tell a teacher.

The 'Internet Safety' button on the home page of the School Intranet links to the CEOP website.

I confirm that I have read and understand this policy.

…….....

OLD BUCKENHAM HALL
A leading co-educational preparatory school for children aged 2-13 years

Agreement for safe and fair use of computer equipment (Middle School)

Introduction

You will all use the computers whilst you are in Years 3 & 4. You may sometimes use the school iPads.

All pupils are asked to read this document with their Teacher. So that everyone at OBH uses the computers and iPads safely and with due consideration for others, we need to have some rules which you must follow.

Using the Computers

- **If I am ever worried about anything I find on the computers or iPads I will tell a member of staff.**

- I will only use the username and password I have been given.
- I will not give my username and password to anyone else.
- I will use the computers sensibly and not touch any of the wiring at the back. When I have finished I will leave the computer tidy for the next person.
- I will only use the Computer Room when allowed to by my teachers or by the duty staff if I am here in the evenings.

Using the Internet

- **If I see anything or receive any messages that concern me, I will tell a member of staff immediately because this will help protect other pupils and me.**
- I will not deliberately search for rude or inappropriate material on the Internet.
- I understand that all my use of the computers is recorded.
- I will not give away any personal information to any sites on the Internet. If I am not sure about this, I will ask a member of staff.
- I will not copy or download work from the Internet and claim it as my own.

Using Office 365 e-mail

You will be given an OBH e-mail address while you are in the Middle School. If you are a boarder, you might like to use it to contact your parents and family.

- I understand that I will only send messages using my own email address.
- **If I receive an email that I am worried about or that I find unpleasant, I will not delete the email but will tell my Form Teacher or Miss McGlade as possible**

- I will only e-mail people I know. For my own safety I will not give any personal details such as my email address, home address or phone number to people I do not know.
- I will not use the email system to send games or inappropriate material to other people.
- I understand that if I use my school email / Office 365 account from home or elsewhere, I must still follow these rules.

The OBH Way

- I understand that we must use computers and other devices responsibly, safely and always with respect for others
- I understand that if I deliberately disobey these rules I may receive a punishment.

Remember that these rules are for your own safety.

If you are worried about anything, you must tell a teacher or your parents.

The 'Internet Safety' button on the home page of the School Intranet links to the CEOP website.

I confirm that I have read and understand these rules.

…….....

Acceptable Use Policy for pupils using their personal laptop at school

Introduction

You have been allowed to use a laptop at school. Mrs Gillott has given permission for this and you are able to use your laptop during the school working day to help you with your work. You will be aware of the school Acceptable Use Policy (AUP) and please remember that it always applies whenever you are using any computer at school.

Additionally the following rules apply:

Using my laptop

- **If I am worried about anything I find on my laptop, I will tell a member of staff.**
- I understand that I am using my laptop to help me with my school work. Use of it for playing games or any other use not connected with my school work is not allowed.
- I may access the Internet on my laptop at school but only when supervised in lessons or prep time. I understand that sites that I visit at school are recorded.
- I understand that the ICT staff will help me get my laptop connected to the school network and will help me set up Office 365 so that I can access my email and cloud storage and also transfer files to my storage area on the network. I will be shown how to print my work when this is necessary.
- My laptop must be kept in Mrs Gillott's room when I am not using it, and not left around the school where it might be damaged. Mrs Gillott and the ICT staff will be able to help when your laptop needs charging but you are responsible for making sure that it has enough charge for the day.
- The ICT staff are able to help you if you have problems with your laptop at school so please ask them for assistance if necessary.
- I have read the school Acceptable Use Policy.

School Code of Conduct

- I understand that deliberate misuse of the ICT facilities may result in action being taken under the school Code of Conduct.

Remember that these rules are for your own safety.

If you are concerned about anything, tell a teacher.

The 'Internet Safety' button on the home page of the School Intranet links to the CEOP website.

I confirm that I have read and understand this policy.

……..……..

Measures in place to support the policies:

The Acceptable Use Policies protects all parties by clearly stating what is acceptable and what is not. This is discussed and explained to all pupils at the start of the school year, initialled and then kept in a file within the ICT department.

Education

All pupils joining the school receive CDT lessons. A key component of these lessons is to achieve an understanding of the important issues of e-safety contained within this policy. We not only look at what is acceptable/unacceptable behaviour, but we also discuss the consequences of these actions. Material is age-appropriate and much of the content is based on the CEOP recommendations. Any member of staff using the ICT Room or the school laptops should remind children of best practice on a regular basis.

Whole Staff

It is the responsibility of the ***whole*** staff to be vigilant at all times, not just specific members of staff. This includes trips out, residential trips, break times, lessons, and after school. We regularly remind staff of the need for this duty.

Parents

The school is keen to educate parents/guardians and our aim is to organise regular workshops, sessions etc. This is a crucial link to helping keeping children safe, as issues can occur when pupils are at home and not using the school systems.

Other

Assemblies, workshops, PSHE lessons and form groups all address cyber-bullying, safe use of the Internet and appropriate use of technologies.

Procedures, Monitoring and Sanctions

If any member of staff has a suspicion that material concerned with an incident – involving staff or pupils - may contain child abuse images, or if there is any other suspected illegal activity, The Headmaster & DSL should be contacted immediately and the matter must be reported to the police under local Safeguarding arrangements.

Other Incidents involving contravention of the AUPs - and any other concerns – should be reported to the E-Safety Lead and / or the Senior Deputy Head. Most initial offences will be dealt with by the e-Safety Lead in conjunction with the Senior Deputy Head, and the removal of computer access may result. In such circumstances, The DSL, Form Teachers / Tutors will be informed and parents/guardians may be notified. An entry will be made in the e-Safety log and CPOMS.

Offences that are more serious or repeated abuse of the Acceptable Use Policy by a pupil will be dealt with by the Headmaster in conjunction with the DSL, e-Safety Lead and the Senior Deputy Head. The removal of computer access may result and other sanctions may be applied. In such circumstances, the pupil's parents/guardians will be notified and may be asked to come into school. An entry will be made in the e-Safety log and CPOMS.

Should Incidents of Sexting involving OBH pupils occur, they will be considered a Safeguarding issue and dealt with by the DSL, according to the guidelines Sharing nudes and semi-nudes: advice for education settings working with children and young people (updated March 2024)

Under circumstances when abuses of ICT constitute a safeguarding concern the DSL will take appropriate action in conjunction with the E-Safety Lead.

The e-Safety Log

This is kept up to date by the DSL/ e-Safety Lead. It is monitored by the Governor with responsibility for Safeguarding. The log is maintained electronically.
The keyword system can generates a significant number of false positives – where use of the keyword has been accidental (please see page). The Head of CDT will check the log regularly and will investigate further and report to the DSL if there is a Safegarding concern. Many first offences will result in a warning but repeat / serious offences will be recorded in the school's iSAMS / CPOMS system and dealt with under the school's code of conduct—they will also be entered in the official e-Safety log.

Monitoring and review of the e-Safety Policy

This policy is monitored by Safeguarding Team. The policy will be reviewed as a result of an incident, changes in guidance, or on an annual basis.