e-Safety Policy

Revised: August 2020

Review date: August 2021

This policy should be read in conjunction with the OxSFC COVID-19 policy that overrides the guidelines/procedures in this policy, where appropriate. The guiding principle will always be to maintain the health and safety of all stakeholders.

Introduction

The College's e-Safety policy applies to day students and boarders. It is interpreted and applied age-appropriately. It takes account of the DfE's 2014 paper **Cyber bullying: advice for head teachers and College staff**, **Working Together to Safeguard Children 2018** and **Keeping Children Safe in Education 2020**. This policy should be read in conjunction with the Child Protection policy.

Oxford Sixth Form College believes that the Internet is a vital tool for modern education; it is a part of everyday life for academic work and social interaction in the College, and consequently the College has a duty to provide students with quality Internet access as part of their learning experience. Given that they also use the Internet widely outside of College, students need to learn how to evaluate online information and to take care of their own safety and security as part of their broader education.

The use of technology has become a significant component of many safeguarding issues. Child Sexual Exploitation (CSE); radicalisation; sexual predation; technology often provides the platform that facilitates harm.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

The purpose of Internet use in College is to raise educational standards, promote student achievement, develop initiative and independent learning, foster imagination and knowledge, support the professional work of staff and enhance the College's management functions. For boarders, and in particular international boarders, the Internet is, along with the mobile phone, also a crucial means of keeping in touch with home and family.

The aims of this policy are to:

- Enable students to take full advantage of the educational opportunities provided by e-communication.
- Inform and educate students as to what constitutes appropriate and inappropriate internet usage.
- Safeguard students and to protect them from cyber-bullying and cyber-abuse.
- Help students take responsibility for their own online safety.
- Ensure that the use of information and materials sourced from the internet by staff and students complies with copyright law.
- Help students use technology safely and appropriately.

Definitions

Cyberbullying
Cyberbullying, or online bullying, can be defined as the use of technologies by an individual, or by a group of people, to deliberately and repeatedly upset someone else.

E-Safety
Limiting the risks to which students are exposed, when using technology, so that all technologies are used safely and securely.

Guidelines

Student responsibility
Students are responsible for their actions, conduct and behaviour when using the Internet, at all times, in and outside of the College.

Use of technology should be safe, responsible and legal. Any misuse of the Internet, inside or outside of College, will be dealt with under the College's behaviour policy.

Sanctions will also be applied to any student found to be responsible for any material on his or her own or another website e.g. Facebook, that would be a serious breach of College rules in any other context. (See the Promoting Good Behaviour policy).

Online activities which are not permitted at the College

Retrieve, send, copy or display offensive messages or pictures.

- Use obscene, fundamentalist or racist language.
- Harass, insult or attack others.
- Damage computers, computer systems or computer networks.
- Violate copyright laws.
- Use another user's password to log into their account.
- Trespass in other user's folders, work or files.
- Use the network for commercial purposes.
- Download and install software or install hardware onto a College computer, whether legitimately licensed or not.
- Intentionally waste limited resources, including printer ink and paper.
- Use the College computer system or the Internet for private purposes unless the Principal has given express permission for that use.
- Copy, save or redistribute copyright-protected material without approval.
- Subscribe to any services or order any goods or services unless specifically approved.
- Play computer games unless specifically approved by the College.
- Use Internet chat rooms.
- Use the network in such a way that its use by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages).
- Publish, share or distribute any personal information about any other user such as home address, email address, telephone number, *etc.* See the College Data Protection policy.
- Use College computers or the Internet for financial gain, gambling, political purposes or advertising.
- Engage in any activity that breaks a College rule.

Bullying

Students must not use any technology to bully others either inside or outside the confines of College buildings. Bullying incidents involving the use of technology will be dealt with under the College's anti-bullying policy.

If a student thinks s/he or another student has been bullied in this way, they should talk to a member of staff about it as soon as possible.

If you are bullied online

You should never respond or retaliate to cyberbullies. You should report incidents appropriately and seek support from your line manager or a senior member of staff. Students should seek support from their Senior Tutor or a senior member of staff.

You should save evidence of the abuse; take screenshots of messages or web pages and record the time and date.

Where the perpetrator is known to be a current student or colleague, the majority of cases can be dealt with most effectively through the College's own disciplinary procedures.

Where the perpetrator is known to be an adult, in nearly all cases, the first action should be for a senior staff member to invite the person to a meeting to address their concerns. If they have a reasonable complaint, make sure they know how to raise this appropriately.

You can request that the person removes the offending comments. If they refuse, it should be an organisational decision about what to do next – either the College or you could report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers or support from other agencies such as The UK Safer Internet Centre.

If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you or a representative from the College may consider contacting the local police. Online harassment is a crime.

Responses to cyber-bullying

Cyber-bullying can be defined as "the use of Information Communication Technology, particularly mobile phones and the internet, deliberately to hurt or upset someone." (DCSF 2007).

Many young people and adults find using the Internet and mobile phones a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively.

When children are the target of bullying via mobiles phones, gaming or the internet, they can often feel very alone, particularly if the adults around them do not understand cyber-

bullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, College staff and parents and carers understand how cyber-bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

The DfE and Childnet have produced resources that can be used to give practical advice and guidance on cyber-bullying. See: http://www.digizen.org/cyberbullying

Cyber-bullying (along with all forms of bullying) will not be tolerated at OxSFC, whether the bullying originates inside or outside the College. Activities conducted outside of College premises and outside of College hours that in our opinion constitute cyber- bulling will also be covered by this policy. Instances of Cyber-bullying will be dealt with according to the College's anti-bullying policy. All incidents of cyber-bullying reported to the College will be recorded.

The College will take reasonable steps to identify the person(s) responsible for any instances of cyber-bullying such as examining system logs, identifying and interviewing possible witnesses and contacting the service provider and the Police if necessary.

Sanctions may include:

- Informing parents/guardians.
- The withdrawal of privileges *e.g.* to bring a phone into College or to use the College internet facilities.
- The person(s) responsible being instructed to remove any material deemed to be inappropriate.
- Temporary or permanent exclusion in the most serious cases.
- The Police being contacted if a criminal offence is suspected.

Abuse

If there is a suggestion that a student is at risk of abuse from his or her involvement on the Internet, the matter will be dealt with under the College's policies for Safeguarding and Child Protection. If any student is worried about something that they

have seen on the Internet, they must report it to a member of staff about it as soon as possible.

Responses

All e-safety complaints and incidents will be recorded by the College on the Serious Incident Log, together with actions taken.

Breaches of regulations will be dealt with according to the College's Promoting Good Behaviour and Child Protection procedures. Any instances of cyber-bullying will be treated in accordance with the College's anti-bullying policy and will be dealt with thoroughly and appropriately.

In such cases, the Principal will apply any sanction that is deemed appropriate and proportionate to the breach including, in the most serious cases, asking a student to leave the College.

Misuse may also lead to confiscation of equipment in accordance with the College's policy on behaviour and discipline.

Security

Staff and students should not leave a computer or any other device logged in when you are away from your desk. Enabling a PIN, passcode or encrypting a device is an important step to protect against losing personal data and images (or having them copied and shared) from a mobile phone or device if it is lost, stolen, or accessed by others. For further information please see the Data Protection policy.

It is a good idea to keep a check on your online presence – for example by typing your name into a search engine. If there is negative content online it is much easier to deal with this as soon as it appears. The *UK Safer Internet Centres Reputation* mini-site, https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/professional-reputation has more information on this.

Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos. Consider your own conduct online; certain behaviour could breach your employment code of conduct. Discuss these same issues with close family, friends and colleagues, as you could become a target if they do not have security and privacy settings in place.

Members of staff should not accept friend requests from students past or present. Be aware that your social media friends may also be friends with students and their family members and therefore could read your post if you do not have appropriate privacy settings.

Do not give out personal contact details to students. If students need to contact you for any reason always use your College's contact details. On College trips, staff should have a College mobile phone rather than having to rely on their own. See the College Trips policy.

Staff and students should use their College email address for College business and personal email address for your private life; do not mix the two. This includes file sharing sites; for example Dropbox and YouTube.

Principles and acceptable use of ICT

Monitoring and usage

Users should be aware that the College monitors and can track and record the sites visited and any searches made on the Internet by individual users. The IT Manager runs a report every month and records the user and type of website that has been visited during that month whether it's through Wi-Fi or Ethernet. Actions are taken in accordance with this policy.

The College has appropriate filters in place to restrict access to inappropriate content, sites known to be detrimental to young people and the Dark Webb. Phrase filters prevent students and staff from searching websites related to terrorism, far right extremist groups, pornography and other inappropriate sites.

We would advise parents that we provide filtered access to the Internet for students but they should also be aware that, with emerging and constantly changing technologies, there is no absolute guarantee that a student will not be able to access material that would be considered unsuitable. The chance of just coming across such content is highly unlikely, but it obviously increases in direct proportion to the amount of time and effort an individual puts into their search. Anyone inadvertently coming into contact with such material must contact a member of staff immediately. When using the Internet, all users are expected to comply with all laws and government regulations concerning copyright, libel, fraud, discrimination and obscenity.

All College staff members are expected to communicate in a professional manner consistent with the guidelines in the Staff Code of Conduct.

Access to the Internet in the College is given to students on the understanding that they will use it in a considerate and responsible manner. It may be withdrawn if acceptable standards of use are not maintained.

Managing email

Email is an immensely valuable tool for educational communication. However, it can also be a channel for cyber-bullying, abuse and defamation. Spam, phishing and virus attachments can also make email dangerous. As a consequence:

- Students may only use approved email accounts on College computers
- Students must notify a member of staff if they receive offensive email
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone not known to them without specific permission
- Social email use during the College day can interfere with learning and will be discouraged
- Email sent to external organisations should be written carefully and authorised before being sent, in the same way as a letter written on College headed paper
- Sending or replying to anonymous messages and chain letters is not permitted
- Staff should use College email accounts to communicate with students on professional matters only.

Managing Social Media and Social Networking sites

Parents, students and teachers need to be aware that the Internet has emerging online spaces and social networks which allow unmonitored content to be published. Students should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. Examples include: blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chatrooms, instant messaging and many others.

The College will control access to social media and social networking sites from its own computers because of the potential for harm inherent in such sites, particularly when used by younger students.

Students are advised never to give out personal details of any kind which may identify them and / or their location. Examples include real name, address, mobile or landline phone numbers, College attended, Instant Messaging (IM) and email addresses, full names of friends/family, specific interests and clubs, etc. Similarly students are advised not to place personal photos on any social network space. They should think about how public the information is and consider using private areas.

Staff official blogs or wikis should be password protected. Staff **must not** run social network spaces for student use on a personal basis.

Students should be advised on security, encouraged to set passwords and to deny access to unknown individuals and be instructed in how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private. Students are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory. Posts that, in the reasonable opinion of the College, could be deemed offensive or defamatory to individuals or to the College will be regarded as a serious breach of discipline and will be dealt with in the context of the College's behaviour policy.

Managing mobile phones

Students are permitted to bring mobile phones onto College premises but they remain the responsibility of their owners at all times. The College cannot be held responsible for any theft, loss of, or damage to, such phones suffered on College premises. All phones must not be switched on or used for any purpose in any lesson or other formal College occasion unless given clear permission by the teacher. Students may not bring mobile phones into examinations under any circumstances.

Phones may not be used to bully, harass or insult any other person inside or outside the College either through voice calls, texts, emails, still photographs or videos.

Cyber-bullying of this nature will bring severe penalties in accordance with the College's Promoting Good Behaviour policy.

Any misuse of the Internet through Internet-enabled phones, such as downloading inappropriate or offensive materials or posting inappropriate comments on social networking sites, will be dealt with in accordance with the College's behaviour policy.

Phones must not be used to take still photographs or videos of any person on College premises without their express permission. Even if such permission is obtained they must under no circumstances be used to ridicule, harass, bully or abuse another person in any way. Any unacceptable use of mobile phones will be dealt with in accordance with the College's behaviour policy.

The College reserves the right to confiscate for a fixed period the phone of any person contravening these protocols and to forbid them from bringing a mobile phone into College for any length of time deemed appropriate by the College.

Managing alternative communication platforms

From time to time the college will permit the use of alternative communication platforms to communicate between the College, the boarding houses, the staff and with students. These will include but are not limited to Instagram, Facebook, Twitter, LinkedIn and WhatsApp. Students will be invited to partake on a voluntary basis and must agree to the terms of use as set out by each of these platforms. For any platforms which the student chooses to join the responsibility will be theirs to familiarise themselves with the terms of use of the platform, these often relate to image control, data capture and data storage.

Oxford Sixth Form College will only join students to a social media group with the student's permission and any groups will be administered by at least two members of staff one to be from our safeguarding team.

Managing photography and video capture on College premises

Use of photographic material to harass, intimidate, ridicule or bully other students or staff members will not be tolerated and will constitute a serious breach of the College rules.

Phones must not be used to take still photographs or videos of any person on College premises without their express permission. Even if such permission is obtained they must under no circumstances be used to ridicule, harass, bully or abuse another person in any way.

Indecent images taken and sent by mobile phones and other forms of technology (sometimes known as 'sexting' or Youth Produced Sexual Imagery YPSI) is strictly forbidden by the College and in some circumstances may be seen as an offence under the

Protection of Children Act 1999 and the Criminal Justice Act 2003. Anyone found in possession of such images or sending them will be dealt with by College authorities. If a student thinks that they have been the subject of 'sexting', they should talk to a member of staff about it as soon as possible.

The uploading onto social networking or video sharing sites (such as Facebook or YouTube) of images which in the reasonable opinion of the College may be considered offensive is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material. In this context it makes no difference whether the images were uploaded on a College computer or at a location outside of the College.

Students, if requested, must allow staff reasonable access to material stored on phones and must delete images if requested to do so in any situation where there is any suspicion such images contravene College regulations.

If the College has reasonable grounds to believe that a phone, camera, laptop or other device contains images, text messages or other material that may constitute evidence of criminal activity, the College reserves the right to submit such devices to the police for examination. Such misuse of equipment will be dealt with according to the College behaviour policy and may involve confiscation and/or removal of the privilege of bringing such devices into College premises on a temporary or permanent basis.

Personal Devices

Students are permitted to bring other electronic devices such as laptops, PDAs, tablet computers and mp3 players onto College premises with permission but they remain the responsibility of their owners at all times. They must keep them with them at all times or in a locked locker and they must ensure that they are appropriately made secure via passwords. The College cannot be held responsible for any theft loss of, or damage to, such phones suffered whilst at College.

No electronic device should be misused in any way to bully, harass or intimidate another person whether through text or images. Any such abuse will be dealt with in accordance with the College's behaviour policy.

No electronic device should contain inappropriate material such as violent or explicit videos or photographs, pornography or any

material that could be considered offensive and / or inappropriate in a College context.

Use of 3G, 4G and 5G

The College has no way of managing the use of mobile data as a service provider e.g. Vodafone, O2 and EE have kept unrestricted internet access for everyone. However, it is expected that staff and students will use the internet responsibly, i.e. not viewing inappropriate content at College. If a member of staff or a student is aware of someone viewing inappropriate content they should report it to a member of the Senior Management Team (SMT).

Anti-Virus Software

All laptops should have appropriate anti-virus software that is regularly updated. All College laptops must be encrypted. With a recommendation that all staff personal laptops, used for College purposes, should also be encrypted. The use of data sticks is discouraged because of the risk of the data stick being lost. Images and personal information of students must not be held on data sticks.

Network Access

Students may not access the College network from their laptop or any other mobile device without express permission from a member of staff. No student may use another's laptop without permission from that student. Students may also not connect their personal laptops to the College network via Ethernet cable and they are not permitted to connect to any other hardware without express permission. This includes detaching and attaching College keyboards and the mouse for personal use as this renders College equipment inoperable.

P2P and File Sharing

No computer programs (executables), MP3s, pornography, or copyrighted material may be distributed over the network. This includes the sending of files via email, as well as setting up 'servers' on students laptops and using them as a means of sharing software.

Students should not download copyrighted material or non-shareware programs and should not be using their laptops as a means to view films, images, or graphics which are deemed inappropriate.

Online Chat

Students may not use any chat or collaboration program to communicate with others through the College's computer network

unless a teacher expressly permits them to do so. This includes the use of email during lessons.

Audio
Because computer audio can be distracting, the audio volume on laptops must be muted when used during College time.

Games
Computer games should never be played in class, during study time or lunchtime sessions unless part of a specified homework that is detailed in the student planner or on a VLE. Any game played should be age appropriate and not contain offensive material in the form of images, sounds or graphics. These will be checked by a member of staff. Students will be asked to remove them if they are deemed inappropriate.

Privacy
The College reserves the right to examine the hard drive on a staff or student's personal laptop if there is reasonable suspicion that a computer is being used for inappropriate or dishonourable purposes.

College Owned Computer Hardware
These must only be used under the supervision of a member of staff and must only be used for educational purposes. The uploading of inappropriate material such as images, software and graphics is forbidden and this includes the doctoring of screen savers and backgrounds.

Consequences
Students found in breach of these rules may have their Internet privileges removed, the privilege of using their laptop, netbook, PDA or tablet PC at College removed either permanently or temporarily, and, depending on the seriousness of the breach, they may also have other sanctions imposed in accordance with College's behaviour policy.

Further sources of information
The DfE guidance and advice can be found at:

https://www.gov.uk/government/publications/preventing-and-tackling-bullying

Advice
If a student, parent or member of staff is unsure about a situation or events, several organisations will speak in confidence to advise what would be the best thing to do:

NSPCC

01793 683100

ChildLine
0800 1111

CEOP
Gives advice on how to operate safely on the web, in particular the **thinkuknow** pages: http://ceop.police.uk/

Organisations

Advisory Centre for Education (ACE)
0808 800 5793

Children's Legal Centre
0845 345 4345

Kidscape Parents Helpline
0845 1 205 204 (Mon-Fri 10am-4pm)

Parentline Plus
0808 800 2222

Youth Access
020 8772 9900

Bullying Online
www.bullying.co.uk

The Anti-Bullying Alliance (ABA)
The ABA brings together over 100 organisations into one network to develop and share good practice across the whole range of bullying issues.

Kidscape
A charity established to prevent bullying and promote child protection. They offer advice for young people, professionals and parents about different types of bullying and how to tackle it. They also offer specialist training and support for College staff, and assertiveness training for young people.

ChildNet International
Offer specialist resources for young people to raise awareness of online safety and how to protect themselves.

Contact details of agencies outside the College

Emergency
If someone is in immediate danger always phone **999** or **112** and report the matter to the Police. The local Police has a specialist team who deal with protecting vulnerable people: Detective Superintendent Nora Holford is Head of PVP

Oxfordshire Social Services

- If anyone is concerned that a child is being abused they can phone Social Services Single Point of Access Team on **01865 902515**
- Outside of office hours phone the Emergency Duty team **0800 833 408.**
- LCSS central team: 0345 2412705 (this should be the first port of call unless a child is in immediate danger. In that case call the MASH team
- MASH team 0345 050 7666

The Local Authority Designated Officer (LADO) is: Alison Beasley **01865 323457**

Oxfordshire Local Safeguarding Children Board is at:

Oxfordshire Safeguarding Children Board
Oxfordshire County Council
County Hall - 3rd floor
New Road
Oxford
OX1 1ND

Tel: 01865 815843
Fax: 0845 605 4165
Email:oscb@oxfordshire.gov.uk
for any general safeguarding issues.

To speak to a local social worker:

Emergency Duty Team
0800 833 408

Oxford (City)
01865 323048

National bodies

The Children's Commissioner
The role of the Children's Commissioner was created by the Children Act 2004 and has been strengthened by the Children and Families Act 2014. Anne Longfield is the Children's Commissioner for England since the 1 March 2015. She has a legal duty to promote and protect the rights of all children in England with a particular focus on children and young people with difficulties or challenges in their lives, and in particular those living away from home, in or leaving care, or receiving social care services. Her work focuses on making sure that adults in charge, or making decisions, listen to what children and young people say about things that affect them.

0800 528 0731 (Monday to Friday, 9am to 5pm)

advice.team@childrenscommissioner.gsi.gov.uk