Online Safety Policy

1. Introduction

1.1 At Wycombe Abbey the use of modern technology is encouraged, particularly to enhance the pupil's academic work, and improve their digital skills and competence. The School recognises that technology plays an enormously important part in the lives of all young people. Current and emerging technologies used in and outside of school include:
Mobile telephones, Tablets, Smart Watches, Smart Devices, Laptop Computers and Desktop Computers

1.2 We teach pupils how to stay safe in an online environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, being targeted by radical, extremist groups, bullying, harassment, grooming, stalking and abuse. They also learn how to avoid the risk of exposing themselves to subsequent embarrassment or damaging future career possibilities.

1.3 This policy is applicable to all those involved in the provision of education and resources in School, and all those with access to or users of the School ICT systems (including staff, pupils, parents, residents, council members and visitors). This policy covers both fixed and mobile internet devices provided by the School, as well as all devices owned by pupils, staff, residents or visitors and brought onto the school premises, or used whilst in relation to school matters whether in or out of school.

1.4 We will deal with Online Safety incidents in accordance with the procedure outlined in both this policy and in associated school policies, such as safeguarding and child protection, pupil behaviour rewards and sanctions, staff behaviour and anti-bullying policies.

2. Objectives

To promote responsible behaviour and use of all those in the School community in using technology whilst taking account of legislative guidance.

3. Roles and Responsibilities

3.1 The School recognises that blocking and barring sites are no longer adequate, although we remain committed to monitoring and filtering access to the internet as appropriate. We teach all in our community to understand why they need to behave responsibly if they are to protect themselves and the community. This aspect is led by the Designated Safeguarding Lead (DSL) and involves the Head of Computer Science, Head of ICT Services and a cross community E-Safety committee.

3.2 The DSL is responsible for ensuring all members of the School community work towards upholding this policy. They keep up to date on current online safety issues and including guidance issued by Department for Education, Bucks County Council, Local Safeguarding Board and other expert bodies. The DSL will advise on online safety policy, review and development, ensure that staff are aware of this guidance, provide staff training, liaise with school technical staff, liaise with the Headmistress or Deputy Head (Pupils) on any investigation and action in relation to online incidents.

3.3 The Bursar, with the ICT Services Department, is responsible for maintaining a safe technical infrastructure and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the hardware system and data. They ensure that users may only access the networks and devices through an enforced password protection approach.

3.4 We are aware of our responsibility to ensure that pupils should not be able to access harmful or inappropriate material through the School IT system. A member of administrative team monitors "Policy Central" a package which helps to identify computer misuse and will identify pupils accessing or trying to access harmful and inappropriate content online. Any findings are reported to the Deputy Head (Pupils) who follows up as appropriate.

3.5 All staff should maintain an awareness of school online safety policies and practices and report any suspected misuse or problem to either the DSL or Bursar as appropriate.

Staff should ensure that all digital communications with pupils, parents and fellow staff are on a professional level. Staff will ensure that pupils understand and follow the Pupils Responsible use of Digital Devices Policy (Appendix A), including the need to avoid plagiarism and uphold copyright regulations. The policy for staff in terms of general rules and use of computers is in line with the Responsible Use of Digital Devices for Pupils policy and is set out in the Acceptable Use of IT for Staff Policy.

3.6 Council members, through the DSL, ensure that the training of staff and pupils is integrated into the overarching approach to safeguarding.

3.7 Residents, Visitors and Community users will be expected to sign an Acceptable Use Agreement before being provided with access to the School IT Systems.

Parents play a crucial role in ensuring that their children understand the need to use the internet/digital devices in an appropriate way. Parents are asked to support the School in promoting good Online Safety practice and follow guidelines. Regular information is provided to parents along with a series of sessions called *Parenting the Teenager*.

4. Child Protection

All staff are made aware of the implications that may arise from sharing personal data, access to illegal and inappropriate material, potential incidents of grooming and cyber-bullying.

All communications with pupils must also be in line with the recommendations made in the Staff Behaviour Policy. Particular note must be taken of the recommendations for use of email and text communications. Internet social networking is not an appropriate method of communication with pupils or former pupils. Staff are advised and regularly reminded to maintain the highest possible privacy settings on any social networking sites that they use and not to post anything that might compromise their own professional reputation or bring the School into disrepute. The DSL regularly provides useful updates on latest technologies and how to maintain privacy settings.

Staff receive regular Safeguarding training and bulletins and are made aware of the importance of reporting any concerning behaviour including pupils' use of the internet.

5. Management of pupil use of 3G, 4G and 5G

We have developed a fast and highly accessible wifi network structure within the School and boarding houses to encourage pupils to access the internet via the School wifi.
However, we recognise that pupils will access the internet using their own 3G, 4G and 5G access and therefore by adopting a culture of responsible behaviour we aim to educate the pupils to behave appropriately irrespective of the method they use to access the internet.
Younger pupils (UIII) have very limited access to their digital devices, currently for a period of time each evening. Devices are handed in before bedtime.

6. Use of school and personal devices

5.1 Staff:

School owned devices, assigned to a member of staff as part of their role, are both password protected, and encryption enabled so that unauthorised people cannot access the content. When they are not using a device staff must ensure that it is locked to prevent unauthorised access.

Staff are permitted to bring in personal devices for their own use and may access the School wifi network.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents / guardians and only in emergencies (where a school device is not available) should staff contact a pupil or parent / guardian using their personal telephone number, email address, social media, or other messaging system. It is sensible to ensure your Line Manager and DSL is aware when this has occurred.

6.2 Pupils:

We allow pupils to use their own devices as teaching and learning tools. Pupils are required to adhere to the Pupil BYOD Policy (Annex B) when using digital devices and their use of the device complies with this policy and the Responsible Use of Digital Devices for Pupils Policy.

We recognise that digital devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a digital device for such purposes, the pupil's parents or guardians should arrange a meeting with Head of Learning Enhancement or Health Centre to agree how the School can appropriately support such use. The Head of Learning Enhancement or Health centre will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

We reserve the right to access a pupil's user-area. personal device or any other form of storage medium eg USB device in their possession if it has grounds to suspect, or evidence of, unacceptable use and breach of the Responsible Use of Digital Devices for Pupils policy.

7. Use of internet, social media and email

7.1 Staff:

Staff should not access social networking sites, personal email, any website or personal email which is unconnected with school work or business, whilst teaching in front of pupils. Such access may only be made whilst not on duty.

Staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the School. See the Social Media Policy in the Staff Handbook.

The School has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the School network and staff email addresses are monitored.

Staff must immediately report to their Line Manager (or HR Department) the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Staff must remain alert to the risk of fraudulent or phishing emails and should report emails they suspect to be fraudulent to the ICT Help Desk.

Any online communications sent must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Wycombe Abbey into disrepute;
- breach confidentiality;
- breach copyright;
- breach the data protection policy;
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion, belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should School pupils or parents be added as social network 'friends' or contacted through social media, until **five years after the pupil has left** the School.

Any digital communication between staff and pupils or parents / guardians must be professional in tone and content.

Under no circumstances may staff contact a pupil or parent / guardian using any personal email addresses. Staff have access to their work email account when offsite, for use as necessary on school business via remote access

7.2 Pupils:

All pupils are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school assignments / research / projects / communicating with fellow students and staff. Pupils should be aware that email communications through the School network and school email addresses are monitored.

There is strong anti-virus and firewall protection and filtering system on our network. Spam emails, certain attachments and certain websites will be blocked automatically by the email system. If this causes problems for school work purposes, pupils should contact IT Help Desk for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to their Housemistress or Head of ICT Services (through the IT Helpdesk)

Pupils are expected to think carefully before they post any information online, repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others. Pupils are reminded of this through school assemblies, tutor sessions, house orders and through academic lessons.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the Head of IT Services or Housemistress. Deliberate access to any inappropriate materials by a pupil will lead to the incident being dealt with under the School's Behaviour, Rewards and Sanctions Policy. Pupils should be aware that all internet usage via the School's systems and its wifi network is monitored.

8. Data Protection

The School takes its compliance with the General Data Protection Regulations seriously. **Please refer to the Data Protection Policy, Data Retention Policy, Privacy Notices and the Staff Acceptable Use of IT Policy for further details.**

Any data breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Data Breach Team – Compliance Manager, Bursar or Head of ICT Services.

8.1 Password security

Pupils and staff have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every six months;
- not write passwords down; and
- not share passwords with other pupils or staff.

8.2 Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Staff and Parents must refer to the Taking, Storing and Using Images of Pupils Policy before taking images that include pupils.

9. Misuse

We will not tolerate illegal activities or activities that are inappropriate in a school context and will report illegal activity to the police and/or the Buckinghamshire Safeguarding Children Partnership (BSCP). If the School discovers that a child or young person is at risk because of online activity, it may seek assistance from the Child Exploitation and Online Protection Centre (CEOP) or other appropriate external agency.

Incidents of misuse or suspected misuse must be dealt with in accordance with the School's policies and procedures, in particular the Safeguarding and Child Protection Policy

The School will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

10. E-Safety Committee

The E- Safety Committee’s purpose is to provide a consultative group that has a wide representation from the Wycombe Abbey community, with a remit to raise and discuss issues regarding online safety within the context of safeguarding.

The Designated Safeguarding Lead takes the lead responsibility for safeguarding and child protection (including online safety), and uses this group to help inform training needs and future technology strategy.

Membership of the committee includes representatives of all stakeholders from the school community including the following:

- Head of Computer Science
- Representation from the staff body – teachers, management and technical support
- Representation from the student body including the House Digital Officers
- Representation from parents
- From time to time other guests may be invited to join the meeting to provide advice and assistance where necessary

The committee endeavour to meet once a term.

11. Responsible Use of Digital Devices for Pupils Policy

At the beginning of every year pupils are asked to sign a copy of the Responsible Use of Digital Devices for Pupils Policy. This is gives clear guidelines on what behaviour is expected of them and sanctions for breaking the code.

12. Complaints

As with all issues of safety if a member of staff, a pupil or a parent / guardian has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the Head of ICT in the first instance, who will liaise with the appropriate Deputy Head and undertake an investigation where appropriate.

Please see the Complaints Policy for further information. Incidents of or concerns around online safety will be recorded and reported to the Designated Safeguarding Lead in accordance with the School's Safeguarding and Child Protection Policy.

Designated Safeguarding Lead	
Updated	February 2020
Next review date	February 2021
Member of Council	SD & S Committee

VERSION ESAF/v12/2020

Related Policies:

- Safeguarding and Child Protection
- Staff Behaviour Policy
- Anti-Bullying Strategy
- Responsible Use of Digital Devices for Pupils
- Data Protection
- Behaviour, Discipline and Rewards
- Privacy Notices – Parents, Pupils, Staff, Residents
- Bring Your Own Devices
- Biometrics

Annex A (As currently used)

Responsible Use of Digital Devices for Pupils

This policy is the result of wide consultation with pupils, parents and staff.

We provide network and cloud access for pupils, including wifi in many areas, with appropriate and regularly updated security monitoring and filtering software installed. However, inappropriate and/or illegal activity is strictly prohibited and any breach of this policy will be taken very seriously. The policy is to be read and signed by every pupil to indicate their understanding of the regulations and their intention to abide by the contents of this policy. It is also taken as an acceptance of the consequences that will occur should they breach the policy. This policy governs school computers, personal computers, laptops, games consoles, mobile phones, smart watches and tablet devices and any other similar technology.

General

- I will not download or install any software on School computers.
- I will ensure my own personal devices and computers have appropriate security and anti-virus software installed.
- I will only log on to the School network/ cloud services with my own user name and password.
- I will follow the School ICT guidelines and not reveal my passwords for the School network or any other websites to anyone else.
- I will ensure that all communication with other pupils and staff is responsible, sensible and appropriate.
- I will be responsible for my behaviour when using the Internet, including resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any material that is offensive or illegal I will report it immediately to a member of staff.
- I will not give out any sensitive personal information such as phone number, address or School name to anyone online.
- I will not arrange to meet someone who I do not already know in person.
- I will not store or use images/videos of other pupils and staff without their permission and knowledge and I will not distribute these in or outside the School (including uploading to any social media websites) without the person's express permission.
- I will ensure my online activity both in School, out of School, on School and personal devices will not cause distress or bring into disrepute Wycombe Abbey, the staff, pupils or others.
- I will not use online sources to explore extremist or radical material or that which promotes a terrorist agenda.
- I will respect the privacy and ownership of others' work online at all times, sticking to copyright policy and not plagiarising.
- I will not attempt to bypass the School filtering system.
- I understand that all my use of the Internet, School network, email and other related technologies can be monitored and logged and can be made available to my teachers and senior staff.
- I will follow the School and House guidelines in regards to using digital devices in the appropriate places and at the appropriate times and, when required, will hand in digital devices to staff to be kept in House.
-

Use of Social Networking Sites (including blogs, vlogs, Twitter, Facebook, Snap chat)

No pupil should:

- Post anything that they would not be happy for a parent or member of staff to read.
- Use any foul, offensive or racist language.
- Post anything that could bring the School into disrepute (including being rude about members of staff, other pupils or the School).
- Publish photographs or videos taken in dormitories,
- Do anything that could damage a person's identity or future career.
- Act without regard to the possible consequences of their actions online e.g. liking or sharing posts created by others that could cause harm.

Bullying

Bullying of any form is unacceptable at Wycombe Abbey. Cyber-bullying is specifically using electronic media to deliberately upset someone else. This may be via posts on social media sites, text or other instant messages or through third-party applications such as Snapchat, Instagram, What'sApp or similar. Pupils should be aware that the School will need to consider the impact of such actions as well as the intention. Unkind comments or messages should not be sent or posted for any reason including attempts at humour.
You are not allowed, for your own protection, to use any anonymous posting sites including but not limited to Sararah, Little Gossip, AskFM, Formspring or Omegle
In line with the School anti-bullying policy we will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil or member of staff, whether in term time or not.

Examples of cyber-bullying are:

- Setting up website pages to invite derogatory comments about others.

- Posting unpleasant or insulting comments via any website about another person, including on social media sites such as Facebook and Twitter.
- Sending vicious, unpleasant or insulting texts or instant messages.
- Posting fake or obscene photographs of another person, comments or other forms of data on websites.
- Hacking into social networking sites of other people and making comments on their profile or circulating material from their pages to others.

Sanctions

Abuse of electronic equipment or breach of any aspect of this policy will result in a range of sanctions in line with the School's Behaviour, Rewards and Sanction Policy and Anti-Bullying policies. After investigation of any incident, an appropriate sanction for the offence, will be determined by Senior Staff.

You can expect any of the following, depending upon the seriousness of the incident;

- Confiscation of your personal electronic device(s) for a period of time.
- Restriction of your access to the School network and/or computers or the Internet.
- School sanctions such as School detention.
- Parental involvement.
- In serious or repeated cases, you can expect the consequences to be more serious, including the possibility of suspension or expulsion.

I have read and understood the Responsible Digital Device Use Policy and agree to abide by it.

Pupil Name:

House: Form:

Signature Date:

Bring Your Own Device Policy

Computers are available for pupils to use both in the main school and in the boarding houses. Many pupils from LIV upwards have their own laptop/tablet. For Junior House, there are different rules and parents receive further advice direct from the Housemistress.

We operate a Bring Your Own Device (BYOD) scheme which allows pupils to use their personal devices, laptop/tablet on the School's filtered network connection, thus providing your child with access to the internet, MyWycombe (our Intranet/VLE), Microsoft 365 and school-shared drives. Pupils need to be mindful that they are required to follow the School's guidance regarding digital technology etiquette. Pupils are not permitted to use digital technology, including BYOD, in certain areas of School and at certain times of the School day.

The BYOD scheme will automatically check devices for anti-virus software and critical updates and, only when an appropriate level of protection is confirmed, will it allow access to the Internet via our network. If the level of protection is insufficient, the user will be informed of the steps that must be taken before trying to access the network again.
The essence of basic support is to enable pupils to use the School's infrastructure. The IT Services Department is committed to supporting pupils' laptops and is able to provide:

- Email support via a helpdesk system
- Basic diagnostics*
- Internet connectivity while on campus
- Software repair**
- Virus/malware removal**

*All equipment must be in English; we are unable to support other languages. Basic diagnostic is a 15-minute assessment of the laptop; additional work may be carried out depending on the resources available.
** If data recovery is required, we shall provide an assessment beforehand, but are unable to provide a guarantee for this type of work. All work carried out will be non-invasive, but any warranty information must be supplied prior to work being carried out. We shall always endeavour to resolve any software issues; however, this is a free service and we accept no liability for any data loss or issues created because of this work, or if we are unable to fix the original problem. We are currently unable to provide any hardware support.

We accept Windows and Apple devices on the network providing they have up to date anti-virus software.

It is essential that both pupils and parents read the School's Online Safety Policy and the Responsible Use of IT Policy for Pupils, which can be found on MyWycombe.

Access to Social Networking Sites

At Wycombe Abbey we have long recognised both the impressive, exciting, educational and social opportunities of the internet and the potential for all – pupils and staff – to come to harm through misuse.

We aim to educate the pupils about how to enjoy the advantages of the Internet within safe boundaries. To this end we have established an E-safety Committee to consider our policies regarding safe use of Internet technologies. This committee includes teachers, pupils and parents. The committee meets regularly and, among other issues, the use of social networking sites is under constant review.

Although we support the use of social networking sites for LIV – UVI pupils and we are constantly educating them on the safe use of these facilities, the committee feels that Junior House should not be given access. The policy of these sites is that users should be 13 years old and Junior House pupils are under this age limit. Also, in a tight community, such sites can create problems for pupils, for example, who do not have as many 'friends' on their site or who simply want to opt out of it altogether. We teach the pupils about ICT safety and the good use of social networking in the Junior House year and then allow access from LIV upwards.

If your child will be joining us in UIII, we would be most grateful if you could discourage them from setting up *Facebook* or other social networking sites before they arrive at Wycombe Abbey as they will not have access whilst in school and we would appreciate your support for the work of our E-Safety Committee.

There are some excellent resources:

https://www.ceop.police.uk/safety-centre/	CEOP - Child Exploitation and Online Prevention command
https://www.thinkuknow.co.uk/	Think U Know? - CEOP's advice on online safety
https://www.saferinternet.org.uk/	UK Safer Internet Centre
https://www.internetmatters.org/	Internet Matters
https://educateagainsthate.com/	Educate Against Hate - advice on protecting children from extremism and radicalisation
https://www.gov.uk/government/organisations/uk-council-for-internet-safety	UK Council for Internet Safety (UKCIS)
https://www.barnardos.org.uk/rusafebucks.htm	Barnardos R-U-Safe? (support for CSE/Grooming)
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/	NSPCC Online Safety
https://tosdr.org/	Terms of Service: Didn't Read - website containing simplified versions of the Terms of Service for popular websites and Apps