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
All staff and members of council will receive safeguarding training (including online safety) at induction and updated annually. A whole School approach to online safety is adopted.

1.2 Keeping Children Safe in Education (2022) states:
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; and
- commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

1.3 Pupils are taught 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 are advised on the use of only age appropriate Apps. They also learn how to avoid the risk of exposing themselves to subsequent embarrassment or damaging future career possibilities. DfE advice is followed, along with guidance from UK Council for Internet Safety (UKCIC).

1.4 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. This policy and online safety measures are reviewed annually.

1.5 The School 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 Code of Conduct and Anti-bullying.

2. Objectives

To promote responsible behaviour and use by all those in the School community in using technology whilst taking account of legislative guidance and referring to the following guidance including:

- Keeping Children Safe in Education (Sept 2022)
- Teaching online Safety in School (July 2019)

- Sharing nudes and semi-nudes: advice for education settings working with children and young people (Dec 2020)
- The use of social media for on-line radicalisation (July 2015)
- Relationships education, relationships and sex education (RSE) and health education (Sept 2021).

3. Roles and Responsibilities

3.1 The School recognises that blocking and barring sites are no longer adequate, but remain committed to monitoring and filtering access to the internet as appropriate. All staff and pupils are taught 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, 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.

The DSL leads on safeguarding and child protection training (including online safety). The training is regularly updated, and at least annually. (See Safeguarding and Child Protection Policy for further information)

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 or two-factor authentication approach as appropriate.

3.4 The School has measures in place to ensure that pupils should not be able to access harmful or inappropriate material through the School IT system. The School use both internet filtering and, on pupil-owned School-managed devices, software called "Smoothwall" and "Senso" that helps to identify computer misuse and will identify pupils accessing or trying to access harmful and inappropriate content online. The Director of Safeguarding and Pupil Welfare receives a report of all concerns related to online usage and implements follow up strategies 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 as outlined in the Staff Code of Conduct. Staff will ensure that pupils understand and follow the Responsible use of Digital Devices for Pupils (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 and their own training, ensure that the training of staff and pupils is integrated into the overarching whole School approach to safeguarding.

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

3.8 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 aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. Children can also abuse their peers online, this can

take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content. All 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. All staff follow the reporting guidance set out in the Safeguarding and Child Protection Policy should they be concerned about a pupil.

All communications with pupils must also be in line with the recommendations made in the Staff Code of Conduct. Particular note must be taken of the recommendations for use of email and text communications. Online social networking is not an appropriate method of communication with pupils or former pupils (Seniors).

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.

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

The School have developed a fast and highly accessible WiFi network structure within the teaching areas, community spaces and Boarding Houses to encourage pupils to access the internet via the School WiFi. However, pupils will access the internet using their own 3G, 4G and 5G access and therefore by adopting a culture of responsible behaviour the aim is to educate pupils to behave appropriately irrespective of the method they use to access the internet.

Younger pupils (UIII and LIV) have limited access to their mobile telephones and are not permitted to use them during the School day. For example, telephones are limited to a period of time each evening. For all boarders from UIII to UV, devices are handed in before bedtime. Pupils in the Sixth Form are permitted to keep their devices overnight.

6. Use of School-owned and personal devices

6.1 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 need to contact a pupil or parent / guardian using their personal telephone number, email address, social media, or other messaging system. If this occurs, Staff must ensure their Line Manager and DSL is aware.

6.2 Pupils

Pupils may use their own devices as teaching and learning tools. Pupils are required to adhere to the Digital Devices 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.

The School recognises 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.

The School reserves the right to access a pupil's user-area, personal device or any other form of storage medium e.g. USB device in their possession if there are 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. Staff should also be aware that as part of Safer Recruitment in Education shortlisted candidates for positions have their online profile searched and any information found online may form part of the applicants interview.

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. If the message is from a pupil then staff must alert the DSL immediately.

Staff must remain alert to the risk of fraudulent, trick or phishing emails and should report emails they suspect to be unsafe to the IT 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 the pupil has left the School. Staff are permitted to accept LinkedIn requests from former pupils, but may not initiate the connection and should be aware that the preferred form of communication remains through School e-mail or Seniors network.
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 the School network and by remote access. Access is via a personal login, which is password protected. This official School 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 the School 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 Deputy Head (Pupils).

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 such as Wellbeing.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the Head of ICT 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 UK General Data Protection Regulations and Data Protection Act 2018 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/near misses, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Data Breach Team – Head of Compliance, Bursar or Head of ICT Services – this can be reported via the Staff Handbook.

8.1 Password security

Pupils and staff have individual School network logins, email addresses and storage folders. 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 use the same password as their own email accounts;
- not write passwords down; and
- not share passwords with anyone else, including but not limited to other pupils, staff members, parents, visiting professionals.

8.2 Two-Factor Authentication

Some School software programmes require a second layer of authentication. A code generator will be available via an App on a mobile devise. This must be used at all times where prompted to use.

8.3 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 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. Remote Teaching and Learning

9.1 Recording of lessons

Staff may record lessons for the purposes of sharing with pupils who are unable to attend at the set time. This is not standard practice and decisions about when a lesson will be recorded for an absent pupil will be discussed and agreed in advance with the Deputy Head (Academic). Staff will be provided with training on the recording of lessons and location for secure publishing of the recording for pupils.

Staff should announce to pupils at the start of the session that it will be recorded for the benefit of those pupils unable to attend. (If all pupils are present there is no need to record.) Inform pupils the recording will be deleted once all absent pupils have viewed the recording.

Either instruct all pupils to turn off their cameras and mute their microphone or just those who don't wish to be in view. If they wish to ask a question, they can do this through the chat function.

Remind pupils that lessons must not be downloaded onto their devices, copied or published by them. (This is to protect the teachers' privacy and professional reputation.)

The recording of live lessons will be done in TEAMS or ZOOM and a copy of the lesson will be retained in TEAMS for the Term in which it was recorded, or until there is no further requirement for pupils to view it. It must then be deleted at the end of the Term. (This is important for Staff Privacy too.)

Pre-recorded lessons by staff can be produced in TEAMS or ZOOM and should be stored in the secure area provided for School recordings, Zoom Cloud, SharePoint or Planet E- Stream. Each Head of Department must decide with their staff members whether the lesson can be retained for future use for the benefit of later training. (Again, this is for the staff member privacy rights.)

9.2 One to One lessons and meetings with pupils

Parents will be provided with the guidance that there could be an adult in the room for the individual lesson, but this is not a requirement. Line managers must be invited to be included in the lesson invite via TEAMS and they should drop in at any point. There is no recommendation that these lessons are recorded. If you wish to record the lesson please discuss with the Director of Safeguarding and Pupil Welfare.

10. Misuse

The School 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, such as cyberbullying and consensual and non-consensual sharing of nudes and semi nudes images and videos 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 Strategy.

11. E-Safety Committee

The E- Safety Committee's purpose is to provide a consultative group that has a wide representation from the School 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:

- 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.

12. 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 gives clear guidelines on what behaviour is expected of them and sanctions for breaking the code.

13. 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 Services 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.

Related Policies

Safeguarding and Child Protection
Staff Code of Conduct
Anti-Bullying Strategy
Acceptable Use of IT - Staff
Responsible Use of Digital Devices for Pupils
Data Protection
Behaviour, Discipline and Rewards
Privacy Notices – Parents, Pupils, Staff, Residents
Digital Devices
Biometrics
Social Media Policy

Annex A

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 across the School site, with appropriate and regularly updated security monitoring and filtering software installed. The School-managed, pupil-owned devices have Smoothwall and Senso software installed on them to allow for improved identification of vulnerable pupils and poor use of devices. Should either of these softwares highlight concerning behaviour, a converastion will be had between the pupil and an appropriate member of staff, such as a Housemistress or, in some cases, the Director of Safeguarding and Pupil Welfare. 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.

Digital Device Guidelines for Email

- Always use your Wycombe Abbey email address for School communications. It is expected that you check your email at least once per day.
- When emailing members of staff, pupils should maintain a formal tone, sign off with an appropriate salutation and include a subject line.
- When emailing members of staff, pupils should always copy in another member of staff, such as Tutor or Housemistress. Staff will do the same when they write to pupils.
- Staff will respond as soon as they can to an email during term time but replies may not be instant. Please note that not all staff are in School every day and that staff may not reply to emails during the School holidays.

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 ensure that my own personal device is never left unlocked and unattended.
- I will adhere to the guidelines set out in the Wycombe Abbey Digital Devices Policy if my device is a Wycombe Abbey Digital Device.
- I will only log on to the School network/ cloud services with my own user name and password.
- I will 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 accessing age appropriate 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 and will use Two-Factor authentication where ever possible.
- 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.
- I will only use my device in an appropriate manner during lessons.

Use of Social Networking Sites

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).
- Create a social media using the School name, or variations of, without the prior written consent of the Headmistress.
- Publish photographs or videos taken in dormitories,
- Publish photographs or videos including images of other pupils or members of staff without their consent
- 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.

Child on Child Abuse, including Bullying

Wycombe Abbey adopts a zero tolerance stance to bullying of any form. 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, WhatsApp 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.

In line with the School Anti-bullying Strategy 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.

Pupils must not engage in any behaviour, either in person or online, that is considered to be abusive towards another pupil. This includes, but is not limited to Bullying, including cyber-bullying, and consensual and non-consensual sharing of nudes and semi nudes images and or videos.

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:

Annex B

Digital Device Policy

All pupils are encouraged to have either their own choice of laptop/tablet or a Wycombe Abbey recommended digital device. Computers are available for pupils to use in the main school.

The School allows pupils to use their personal devices, laptop/tablet on the School's filtered network connection, thus providing pupils with access to the internet, SharePoint (our Intranet/VLE), Microsoft 365 (including TEAMS) 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, in certain areas of School and at certain times of the School day.

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

The essence of basic support is to enable pupils to use the School's infrastructure. The ICT 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.

It is essential that both pupils and parents read the School's Online Safety Policy and the Responsible Use of Digital Devices Policy for Pupils.

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.

Pupils are educated about how to enjoy the advantages of the Internet within safe boundaries. To this end an E-safety Committee has been established to consider 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.

Pupils are educated in the age ratings for social networking sites, and are reminded that they should not sign up for an account on any social networking site where they are deemed too young by the allocated age rating.

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 listed below and also in *KCSIE Sept 2022*

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