Abberley Hall
SCHOOL

Abberley Hall E-safety Policy

Last revised: May 2019. *Next review: January 2020*
Author: John Hiles (Head of Computing, e-safety coordinator)

Contents

Policy Statement

We recognise that E-safety is a whole-school issue and responsibility and this policy covers both Abberley Hall Preprep and Prep. Children should receive age appropriate e-safety training from the very youngest to the oldest in the school.
Abberley Hall School recognises that Information Technology, (IT) and the Internet are excellent tools for learning, communication and collaboration. These are accessible within the school for enhancing the curriculum, to challenge pupils, and to support creativity and independence. Using IT to interact socially and share ideas can benefit everyone in the School community. However, it is important that the use of IT and the internet is understood and that it is the responsibility of pupils, staff and parents, to use it appropriately and practise good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Abberley Hall School, Worcester, WR6 6DD
Preparatory School T: 01299 896275 | Pre-Prep & Early Years T: 01299 896101
abberleyhall.co.uk

Scope of this policy

E-safety does not just cover the network resources provided by the school, but all different types of devices and platforms (e.g. Smartphone devices, wearable technology and other electronic communication technologies). The School understands that some adults and young people will use these technologies to harm children. The School has a 'duty of care' towards any staff, pupils or members of the wider school community, to educate them on the risks and responsibilities of e-safety. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy governs all individuals who are given access to the School's IT systems. This could include staff, governors and pupils however, sections of this policy may not be relevant to certain individuals due to their position, job role or subject to the age of the pupil.

Purpose of this policy

To be an aid in regulating IT activity at Abberley Hall

- To educate pupils and staff about e- safety issues and appropriate behaviours so that they remain safe and legal online.
- To provide a good understanding of appropriate IT use that members of the School community can use as a reference for their conduct online outside as well as during school hours.
- To help pupils to develop critical thinking skills to reflect and enable them to keep themselves safe.
- To help users to keep any personal data and information secure.
- To minimise the risks of handling sensitive information.

Roles and responsibilities

The Headmaster (Will Lockett), Designated Safeguarding Lead (Richard Keeble), and Governors (Catharine Hope – safeguarding governor) will ensure that the e-safety policy is implemented and that compliance with the policy is monitored.
The day-to-day management of e-safety in the School is the responsibility of the e-safety coordinator (John Hiles). He will work with the pastoral care team in this regard.
The School will undertake an annual review of our safeguarding procedures and their implementation, which will include consideration of how pupils may be taught about safeguarding, including online safety, through the School's curricular provision, ensuring relevance, breadth and progression.
The School is responsible for reviewing and managing the security of the IT systems that it operates and takes the protection of School data and personal protection of the School community seriously. This means protecting the School network, (as far as is practicably possible), against viruses, hackers and other external security threats. Anti-Virus and Malware protection software will be updated regularly.
The review and provision of services, infrastructure and technologies for the protection of children and staff and sensitive data will be the responsibility of the Network Manager (Nick Corbett) who will work closely with the Head of Computing (John Hiles) to ensure that all that

can be done is done to protect children, the School and sensitive data and that the system is adequately and regularly monitored and updated, including some of the following actions:

- Making sure that unapproved software is not downloaded or installed to any School computers.
- Regularly checking files held on the School network for viruses;
- Enforcing the use of unique user logins and passwords to access the school network.
- Provide encrypted portable media devices for the temporary storage of school data by staff.
- Keeping abreast of new technologies, identifying associated risks and the safeguards that need to be in place to deal with them. Appendix 1.

Communicating School policy

- All individuals with access to the School's IT services will be made aware of the E-safety policy and this policy will be available on the School website for all to access (including parents and visitors), when and as they wish.
- Pupils are required to sign the *Pupil IT Usage Agreement* each term which outlines the acceptable use of technology and the code of conduct when online. (Appendix 2)
- New staff will be required to read and agree to the acceptable use if IT guidelines contained in the *Staff Code of Conduct*. Existing staff may on occasion be required to re-read this document (and sign that they have done so and will abide by it) on a periodic basis or when significant changes have been made.

Promoting good e-safety practice. Staff Pupil & Parental engagement

- The 'SMART' rules and E-safety guidelines will be displayed around the School and in all IT suites.
- E-safety is specifically integrated into the computing curriculum and in certain circumstances where the internet or technology is being used within other subjects, as well as being addressed in the PSHE curriculum. (Appendix 3)
- We will use assemblies and year group meetings to discuss and remind pupils about e-safety topics on a regular basis.
- Special events – e.g. Safer Internet Day (February)
  We have put *Safer Internet Day* on the agenda for the future and will use this annual opportunity to talk about e-safety in assemblies and small groups and through a variety of activities throughout the day.
- We will host parent events periodically where we offer a forum for discussion, dispense advice and talk about online safety and give advice. (Last parent event, June 2017 – presentation by JGH & SMB)
- We will maintain and update an e-safety notice board in the corridor adjacent to the Computer Suites and also put up posters of advice and rules of online conduct in all computer suites. (Appendix 4)

Pupil E-safety Survey (Autumn 2018)

It is important to review the effectiveness of what we teach the children about keeping safe online and we will periodically survey the children to learn about their experiences in the online world at home as well as at school. Our recent anonymous survey of all the pupils (autumn term 2018) revealed that the overwhelming majority of children felt confident that they knew how to behave online and keep themselves safe but also highlighted that a few had experienced some of the risks, such as viewing inappropriate content, receiving unpleasant or unwelcome messages and that there is more that can be done. We are committed to repeating this exercise on a regular basis and using the results to inform the way we help children to remain safe and use technology responsibly.

Published content and the School website

The School website is viewed as a useful tool for communicating School ethos and practice to the wider community. It is also a valuable resource for prospective parents and pupils, current parents, pupils and staff for keeping up-to-date with School news and events, celebrating whole-school achievements, personal achievements and promoting the School. The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the School community.

A team of staff, under the leadership of the Director of Marketing, are responsible for publishing and maintaining the content of the School website. The website will pay respect to intellectual property rights and copyright. Staff and pupils will be made aware of copyright in respect of material taken from the internet.

Staff and Pupils should take care not publish anything on the Internet that might bring the School into disrepute. Any pupil or member of staff is welcome to discuss material with the Director of Marketing, Deputy Heads or Heads.

Colour photographs and pupils' work bring the School to life, showcase pupils' talents, and add interest to publications both online and in print that represent the School. However, the School acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Images of pupils and staff will not be displayed in public, either in print or online, without consent, if the use of the image is considered by the School to be intrusive of privacy.

Related Policies & Documents

- *Code of Conduct for teachers and Staff*
- *Privacy Policy (GDPR)*
- *Laptop Policy & Parent/Pupil usage declaration form*
- *Use of Images & Personal Mobile* Devices Policy

Misuse of technology

Any security breaches or attempts, loss of equipment or data and any unauthorised use or suspected misuse of ICT must be immediately reported to the E-safety coordinator for investigation. If inappropriate material is accessed accidentally, users should also immediately report this to the E-safety coordinator so appropriate action can

be taken. Children that access material that causes them concern should inform a responsible adult immediately and this information should in term be passed on to the e-safety coordinator.
An incident log will be used to monitor what is happening and identify trends or specific concerns.
Proportional sanctions may be applied such as confiscation of equipment, temporary removal of Internet access or the disabling of a Network account.
Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through the School's anti-bullying policy and procedures and any details passed on to the DSL.
If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's child protection procedures (see the School's safeguarding and child protection policy and procedures).

Signed: ……..…… Date: …….. Signed: ……..…… Date:……
Governor Headmaster
Mrs Catharine Hope Mr Will Lockett

This is an all School Policy including Prep, Pre-Prep, EYFS, After School Care and Holiday Club

Appendix 1 - Areas of Technology, associated risks and safeguards in place

- **Websites**
  We recognise that the World Wide Web is a rich and invaluable resource and of huge educational benefit to our pupils and the School will endeavour to equip pupils with all the necessary IT skills for them to progress confidently towards senior school. The Internet is used to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions.

  At the same time, we acknowledge that there is a large amount of unsavoury and potentially damaging material from which pupils must be protected. We take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a School computer or device connected to the School network. The School cannot accept liability for the material accessed, or any consequences of internet access unless found to be negligent.

  Access to websites for all pupils and staff is monitored by a Smoothwall filtering server which uses constantly updated and categorised lists of sites which may be unsuitable. In addition to this we add our own custom lists which are reviewed and added to constantly on at least a weekly basis.

  On top of the *Smoothwall* server we run the *Impero* desktop management system which adds an extra layer of security and allows us to monitor pupil activity on the network and alerts us to suspect web searches and attempts to access blocked or harmful content.
  An important protection for our pupils is that they learn to evaluate internet content. This is approached by the School as part of digital literacy across all subjects in the curriculum. Pupils will be taught:

    - to be critically aware of materials they read, and shown how to validate information before accepting it as accurate, (e.g. "fake news");
    - to acknowledge the source of information used and to respect copyright;
    - about the risks associated with using the internet and how to protect themselves and their peers from potential risks;
    - how to recognise suspicious, bullying or extremist behaviour;
    - the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
    - the consequences of negative online behaviour; and how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.

- The School provides e-safety guidance to staff to better protect pupils and themselves from online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development training includes training on online safety together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles within the organisation, legal changes and requirements.

- If staff or pupils discover unsuitable sites then the URL, time, date and content must be reported to the IT Department or any member of staff. Any material found by members of the School community that is believed to be unlawful will be reported to the appropriate agencies via the Head of IT or a member of the Senior Management Team. Regular checks will take place to ensure that filtering services and e-safety processes are in place, functional and effective.

- **Email Communication**
  The School uses email internally for staff and pupils, and externally for contacting parents, and conducting day to day school business and is an essential part of School communication.

  We encourage pupils to communicate with family and friends outside of school via email and all pupils and staff are provided with a Microsoft Office365 account which includes an official Abberley Hall email address. This means that all emails are filtered for unwelcome content and language. Pupils may not access other external personal email accounts while at school. Pupils are given regular reminders of email etiquette, their responsibility for respecting others and what to do if they receive an unwelcome email.

  Pupils are warned not to reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.
  Excessive social emailing can interfere with learning and in these cases, will be restricted.
  Pupils should immediately inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.
  We recognise that pupils' emails may well be private and sensitive in nature but reserve the right to monitor emails, attachments and their contents. However, this will not be contemplated unless we have good reason to suspect that a serious breach of our acceptable use guidelines has taken place or that harmful emails may have been sent or received.
  Staff should be aware of the following when using email in School:
    - Staff should use their School email accounts for school-related matters, contact with other professionals for work purposes and to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people.

    - Emails sent from School email accounts should be professional and carefully written. Staff are representing the School at all times and should take this into account when entering into any email communications.

    - The School permits the incidental use of staff School email accounts to send personal emails if such use is kept to a minimum and takes place substantially out of normal working hours. The content should not include or refer to anything which is in direct competition to the aims and objectives of the School nor should it include or refer to anything which may bring the School into disrepute. Personal emails should be labelled 'personal' in the subject header. Personal use is a privilege and not a right. If the School discovers that any

member of staff has breached these requirements, disciplinary action may be taken.

- For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by their head of department or a senior member of staff.
- Staff must tell a Senior member of staff if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in School.

- **Firewall & Virus Protection**
  As well as handling the filtering of internet access the *Smoothwall* appliance also acts as our firewall and provides intrusion protection, monitoring and logging.
  Virus protection is provided by *Sophos Antivirus* across the network and is updated on a regular basis.

- **Pupil Computers & Laptops**
  Pupils are only allowed to bring a laptop computer into school if there has been a recommendation from the learning support department that it will assist their learning. Such devices may only be used for lessons or academic purposes, may not be connected to the internet unless in the presence of a member of staff and will be stored in the provided laptop safe when not in use. Laptops will be subject to a safety check by our Network Manager and their usage will be monitored by the Head of Learning support (Catherine Beaumont). Pupils are expected to follow the same guidelines when using their own devices as when using those provided by the school.

- **Tablets, gaming devices, e-readers & smartphones, smart watches & media players**
  Pupils may not bring into school any internet-connected devices (see below for mobile phones). E-readers are allowed but may only be connected to the internet in the presence of staff for the purposes of downloading new and suitable reading matter and should only be used as an alternative to a book, never for playing games etc.

  Access to mobile phones is restricted and for voice-calling parents and guardians only. Mobile phones are stored in the Headmaster's office and must be requested, used for a short time and then returned immediately. It is understood that almost all smartphones will have 4G, Bluetooth & Wi-Fi capabilities. However, pupils must agree that these services will be switched off, and that the phones will not be connected to the internet while at school.
  See *Use of Images & Personal Mobile Devices* policy

- **4G**
  4G is a wireless protocol that allows enabled devices (including mobiles, laptops, tablets ad even smart watches) to connect to a mobile carrier and obtain internet-based services. Pupils may not have access to 4G enabled devices (other than a mobile phone which must have 4G disabled and to which access is strictly monitored).

- **Wi-Fi**
  Wi-Fi is a wireless technology which allows enabled devices to connect to a network and gain access to network resources and associated internet connectivity. Passwords to the school's wireless network are closely regulated and pupils are not allowed to connect devices (including laptop users)

- **Bluetooth**
  Bluetooth is a technology that enables peer-to-peer communication and transfer of data between devices without the need for either a mobile or Wi-Fi network. Pupil's should ideally not have access to such devices but in the event that they are using a mobile phone with Bluetooth they must not switch this on or use this to pass information to one another.

- **Social Media**
  Social Media sites allow users to upload or post images and textual information and view such information posted by others. Users of these platforms can enter into correspondence and exchange information. There are obvious risks for children when using these platforms as they are unregulated, and children can become vulnerable to corrupting, grooming or bullying behaviours.

  While we are aware that children may well be using social media platforms at home and that there is a risk that they may have been exposed to material of an unsuitable nature or put aty risk from strangers, at school these activities are not allowed. All the major social media providers require that children be older than the age of 13 before gaining access to their platform. As all but a handful of our children reach this age while at Abberley we feel it appropriate and prudent not to allow the use of such platforms within the school. Pupils are educated about the risks posed by these platforms and how to protect themselves.

  Staff may use Social Media platforms on their own devices but must do so in line with the Staff code of Conduct and certainly not in the presence of pupils or in such a way as will interfere with their responsibilities at school or compromise their professionalism.

- **Downloads**
  There are many websites that allow files and photographs to be downloaded to the local computer and saved in users' home folder and pupils may do so if these are for academic or legitimate and creative use in line with the *Pupil IT usage agreement*. We reserve the right to routinely scan and check the contents of these folders for disallowed content. (E.g. Games, Videos & Music)

- **Chat rooms & Game chat**
  Many websites and online games allow users and players to communicate freely with one another and this can lead to inappropriate conversations and potential grooming. Pupils are not allowed use such sites while at school and are taught about the dangers of doing

so while away from school.

- **Cameras, photography and Pupil Images**
  Pupils are permitted to take photographs, videos or recordings of classroom-based activities under the direct supervision of their class teacher or TA. The school's own Learnpad tablets allow only authorised websites, games and information to be accessed by the children within school. School cameras will sometimes be made available for supervised projects. Pupils' own cameras may be brought in by permission only for special activities and their use and storage will be strictly supervised by staff.

  Staff should use school equipment for photographing pupils but in the event that these are not available, personal cameras and smartphones may be used appropriately provided the images are quickly transferred to the school's servers and erased from those devices.
  Images are routinely archived onto DVD after 2 years and kept securely. These photos are then erased from the school's servers.

  Images should not be published without parental consent and standards of decency and modesty should be adhered to.

  Some of these issues are covered in more detail in the *Use of Images and Personal Mobile Devices Policy*.

- **Video conferencing**
  Video conferencing is a useful tool particularly for our overseas students to maintain contact with parents or guardians. These sessions are only available by pre-arrangement with staff and parents and a member of staff will supervise the use of equipment, ensure that calls are only made with the designated contact and be present at the beginning and ending of the session.

- **Passwords & security**
  All staff and pupils are required to choose a secure password and taught how to create one that is strong. Pupils are taught that they should not share passwords and should change them if they become known. Staff are required to change their password on a regular basis, and this is enforced from time to time. Pupils must only login in using their own credentials and violation of this will result in sanctions (locking of account for a short time). Users should not leave a computer unattended when logged in and should either log out or lock their screen; this is especially important for staff.
  Staff should never allow pupils to log on using their credentials.

Appendix 2 – Pupil ICT Usage Agreement

Abberley Hall - Pupil ICT Usage Agreement Form

Pupil's Name..... Form .....

Year	*Aut*	*Spr*	*Sum*
1. I will try use school computers for work, learning, research, and making useful things.	☐	☐	☐
2. I will not use school computers purely for entertainment (ie, games, videos etc). Unless given permission.	☐	☐	☐
3. I will treat all ICT equipment with great care.	☐	☐	☐
4. I will not fiddle with computers and other ICT equipment, cables etc.	☐	☐	☐
5. I will only use my own username and password to log onto the network; I will keep this secret.	☐	☐	☐
6. My documents area is for work files and things I have created, NOT things I have download from the internet.	☐	☐	☐
7. I will not be able to attach external storage devices (eg. USB sticks) to school computers. Teachers will do this for me if necessary.	☐	☐	☐
8. I will only print out class-work; I will make sure I have checked it on screen carefully before doing so.	☐	☐	☐
9. I will only access web sites that are educational and suitable for young children. If I accidentally stumble across an unpleasant site I will tell a member of the ICT Staff as soon as possible. I will not visit sites where I can chat to strangers.	☐	☐	☐
10. I will only use the school email system for sending and receiving email while at school; I will only send email when I have a sensible reason, and will never use rude, unpleasant or hurtful language in any message I send.	☐	☐	☐
11. I understand that anything I do on the school system (including email messages and internet access) is stored in a log file and might be looked at by a member of staff;	☐	☐	☐
12. I understand that my computer rights may be removed if I do not abide by this agreement.	☐	☐	☐
Initials			

Appendix 3 - E-safety in the Curriculum

E-safety is covered in PSHE with each year group through discussion and in relation to a variety of topics; E.g.

- Internet Identities – Are people who they say they are?
- Leisure time and a healthy lifestyle
- Bullying, Sexting and Social Media
- Opinions and tolerance,
- Racism and radicalisation

E-safety is covered in the Computing curriculum for each year group using both online and in-house materials as outlined below:

- Year 1 – Secure Logins, Ownership, Privacy and Sharing, Communication technologies - *PurpleMash Unit 1.1 - Online Safety Module*
- Year 2 – Searching, Sharing & Communicating - *PurpleMash Unit 2.2 - Online Safety Module*
- Year 3 – Passwords, Blogs, Is it true? - *PurpleMash Unit 3.2 - Online Safety Module*
- Year 4 – Identity Theft, Malware and Viruses, Plagiarism, Health
  - *PurpleMash Unit 4.2 - Online Safety Module*
- Year 5 – SMART rules for safety, Responsibility, Copyright, permissions, referencing sources, eliability and validation. - *PurpleMash Unit 5.2 - Online Safety Module*
  Year 6 – location tracking, Secure sites, persistence of data, online behaviour, game-time
  - *PurpleMash Unit 6.2 - Online Safety Module*
- Year 7 – Your digital footprint
- Year 8 – Search engines, The web, Hacker & Crackers, Sexting

Appendix 4 - Posters and Handouts

Appendix 5 - Useful Links and Resources

- CEOP - Child Exploitation and Online Protection command

  The Police's Website for information and advice on dealing with online sexual abuse and for making a report.
  https://www.ceop.police.uk/safety-centre/
- NSPCC – National Society for the Prevention of Cruelty to Children

  Resources and advice on e-safety and safeguarding
  https://learning.nspcc.org.uk/

- Internet Matters

  Great resources for online safety issues
  https://www.internetmatters.org

- Childnet International

  International Charity working to improve online safety for children
  https://www.childnet.com
- UK Safer Internet Centre

  Safety tips, advice and resources to help children and young people in the UK stay safe online.
  https://www.saferinternet.org.uk/