SEDBERGH SCHOOL

E-Safety Policy	
Version	2021.1
Effective from	September 2021
Extent of Policy	Sedbergh School
Policy Owner	Senior Deputy Head (Pastoral)
Governor	John Campbell
Review by	September 2022
Frequency of Audit	Annual
Circulation	Teaching Staff Handbook Parents by request
Publication	Website

1 Roles and responsibility for on-line safety and how the E-Safety Policy links with the main Safeguarding Policy

1.1 The E-Safety Policy contributes to the wider Sedbergh Child Protection & Safeguarding Policy and Prevent Policy for anti-radicalisation**.**

1.2 All users need to be aware of the range of risks associated with the use of these internet technologies.

1.3 The Designated Safeguarding Lead (DSL) and the Director of IT have responsibility for ensuring this policy is upheld by all members of the School community. They will keep up to date on current e-safety issues and guidance issued by organisations such as the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Cumbria Safeguarding Children Board. As with all issues of safety at this School, staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

1.4 Sedbergh believes that it is essential for parents/guardians to be fully involved with promoting e-safety both in and outside of School.

1.5 A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be recorded directly to the School's ISAM's system and if necessary directly to the DSL. Should a member of staff encounter anything that causes them concern on a pupils account/personal device they should immediately log this via email to the DSL, and secure the device from any interference from others (without logging off it off or shutting it down). Under no circumstances must they copy the material concerned or forward it via email to any person, nor must they investigate further in any way.

2 Clear guidance on use of technology for all users in all areas of the School and information regarding consequences for abuse of the IT system

2.1 The IT Acceptable Use Policy (see appendix) must be signed by all users of Sedbergh IT.

2.2 Staff will be aware of how to use IT, especially resources, through the Staff Code of Conduct Policy (age appropriate, anti-radicalisation, check before showing, etc).

2.3 KCSIE 2021 defines potential abuse via the internet. Please see: KCSIE 2021.

2.4 Pupils are aware of the consequences of abusing the School internet systems these are laid out in the Behaviour, Rewards & Sanctions Policy.

2.5 Staff are aware of the consequences of abusing the School internet systems these are laid out in the Staff Code of Conduct.

3 Sedbergh has a robust technical infrastructure and provision to safeguard against and monitor inappropriate content and alert the School

4 Detail of how the School builds resilience and develops pupils understanding of e-safety

4.1 The PSHE syllabus looks to heighten awareness, understanding of and resilience to all forms of threat found on line.

4.2 External speakers are brought in to deliver information to pupils (and staff and parents).

4.3 Pastoral staff are given education relating to e-safety which is then passed on through tutor sessions.

4.4 Cross curricular learning is encouraged. IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

4.5 At age-appropriate levels, and usually via PSHEE, pupils are taught to look after their own online safety. From Year 9, pupils are formally taught about online safety in age-appropriate weekly PSHEE lessons, with a view to raising their awareness of issues such as online sexual exploitation, stalking and grooming, and building their online resilience to the associated risks and dangers. PSHEE lessons focus on enabling pupils to understand and identify potentially risky situations online, and on how to report their concerns and seek help if they encounter difficulties online. Advice and support in such situations is always available in School, through Houses, Tutors and Safeguarding Officers (DSL and DDSLs). Pupils learn about relevant laws applicable to using the internet, such as data protection and intellectual property. The CEOP link is permanently present on the School's desktop and pupils are signposted through their PSHEE lessons and other opportunities in School to the advice and guidance it provides.

5 Detail on staff safeguarding professional development that includes online safety

5.1 Child Protection & Safeguarding Policy

5.2 New staff (including supply and support staff) receive information on Sedbergh's E-Safety and IT Acceptable Use Policies as part of their induction. All teaching staff receive regular information and training on e-safety issues in the form of INSET training, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.

5.3 All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following School E-Safety Policy. These behaviours are summarised in the IT Acceptable Use Policy (see appendix) which all account holders must read and electronically accept before they can access our network. When children use School computers, staff should make sure children are fully aware of the agreement they are making to follow the School's IT guidelines.

5.4 Staff should check content of material before using it in teaching and be conscious of the age appropriateness of material in relation to the intended audience. Published age ratings on video content should be observed at all times.

5.5 Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the School community.

5.6 Attention will be given to 'gaming' activities using the internet. It is known that this can be a source of inappropriate material for children and provides opportunities for people to groom vulnerable children.

6 Use of personal devices in School

6.1 **Staff** – School devices assigned to a member of staff as part of their role must have a password/number so that unauthorised people cannot access the content. When they

are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff at Sedbergh School are permitted to bring in personal devices for their own use.

6.2 **Pupils** – All pupils are expected to own a laptop for academic work and guidance is given annually as to the minimum specification considered acceptable for use in School. Advice is also given on security and virus protection and the network scans all devices to ensure they are up to date before allowing connection. Pupils are free to bring in tablets, phones or hybrid technology but only in addition to a laptop.

No mobile phones belonging to pupils are to be used during lessons at School without the express consent of the teacher concerned. Pupils are not permitted to walk around the site using hand held mobile devices. Laptops, tablets and mobile phones remain the responsibility of the child in case of loss or damage.

6.3 **Visitors** – The School's IT Acceptable Use Policy (see appendix) **applies to visitors.**

7 Use of internet and e-mail

7.1 **Staff** – Staff must not access social networking sites, personal emails or any website which is unconnected with School work or business whilst teaching.

7.2 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.

7.3 There is strong anti-virus and firewall protection on the School network and, as such, it may be regarded as safe and secure. Staff should be aware that email communications are monitored. Copies of all emails are retained for future reference should they be needed.

7.4 Fortigate is a security system that allows the School to block any website or internet service that it deems to be unsuitable. There are two Fortigate firewalls, one for each school so that the internet traffic and access to websites can be set at different levels taking into account the age ranges. With over 6,000 blocked sites or associated adverts on a site in an hour, automatic alerts are not enabled, instead log files are checked on a regular basis that tell us who tried to access a site, on what device and where. Any continuing attempts to access and inappropriate site would be reported to the DSL.

7.5 Staff must immediately report to a member of the SMT 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.

7.6 Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring Sedbergh School into disrepute;
- breach confidentiality;

- breach copyright;
- breach data protection legislation; 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 or belief or age;
  - using social media to bully another individual; or
  - posting links or material which is discriminatory or offensive.

7.7 Under no circumstances should pupils be added as social network 'friends'.

7.8 It is recognised that Sedbergh is a close and friendly community and that staff may encounter parents and past pupils/parents on an increasing variety of 'networking platforms'. It is the responsibility of staff to ensure where possible that privacy settings are set to prevent any accidental forwarding of postings ('likes' etc) to current pupils. Staff should be mindful that all use of such platforms carry a professional risk and that the points above apply to personal postings should they be read by someone connected in any way with the School.

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

7.10 **Pupils** – All pupils are issued with their own personal School e-mail addresses. 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 related matters. Pupils should be aware that email communications are monitored.

7.11 There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. Furthermore certain websites are automatically blocked by the School's filtering system. If this causes problems for School work/research purposes, pupils should contact the IT team for assistance.

7.12 Pupils should immediately report to any member of staff 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. Links to both the CEOP and Anti-Bullying services are permanently on the standard School desktop and available to pupils.

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

8 Password security

8.1 Pupils and staff have individual School network logins and storage folders on the server/cloud. Staff and pupils are regularly reminded of the need for password security.

8.2 All pupils and members of staff should:

- use a strong password containing eight characters or more, and containing upper and lower case letters as well as numbers. The network will not accept passwords that do not comply with these criteria.
- not write passwords down and should change them regularly (Sedbergh suggests once every 6 months).
- not share passwords with other pupils or staff.
- staff must use two factor authentication.

9 Data Storage

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

9.2 Staff and pupils are normally expected to save all data relating to their work to either their School OneDrive, SharePoint or network folder, whatever device they are using.

9.3 If staff use personal devices for School work, they must be secured by password access controls and not shared with any other family member. All data must be stored as outlined in 9.2. The School does not encourage the use of removable media USB memory sticks, CDs or portable drives containing any School data. Wherever possible, OneDrive or SharePoint should be sued for the transfer or sharing of data. If it is absolutely necessary to use removeable media which are being sent by post or courier, they must be encrypted before sending. Staff may only take information offsite when it is necessary and required to fulfil their role.

Staff travelling abroad and who need to take any form of School data with them should contact either the Deputy Bursar (Compliance) or the IT Department for advice as the regulations vary depending on the country being visited.

10 Safe use of digital and video images

10.1 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/guardians 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.

10.2 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 (eg on social networking sites).

10.3 Staff and volunteers are allowed to take digital/video images to support educational aims and for marketing purposes, but must follow this policy and the IT Acceptable Use Policy (see appendix) concerning the sharing, distribution and publication of those images. On joining the School parents give their consent for images of their child to be used in this regard.

10.4 Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.

10.5 Photographs published on the School website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images.

10.6 In accordance with guidance from the Information Commissioner's Office, parents/ guardians are welcome to take videos and digital images of their children at School events for their own personal use (as such use is not covered by the Data Protection Act).

11 Complaints

11.1 Please refer to the School's Complaints Procedure.

JMB
August 2021

Appendix

ACCEPTABLE USE OF IT POLICY

This Acceptable Use of IT Policy covers the security and use of Sedbergh School, Casterton, Sedbergh Preparatory School and all other subsidiaries or associated companies or organisations hereafter referred to as 'Sedbergh School', information and IT equipment.

It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all Sedbergh School employees, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to Sedbergh School's business activities worldwide, and to all information handled by Sedbergh School relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Sedbergh School or on its behalf.

Computer Access Control – Individual's Responsibility
Access to the Sedbergh School IT systems is controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Sedbergh School's IT systems.

Individuals must not:

- Allow anyone else to use their user ID/password on any Sedbergh School IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Sedbergh School's IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to Sedbergh School's IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Store Sedbergh School data on any non-authorised Sedbergh School equipment.
- Give or transfer Sedbergh School data or software to any person or organisation outside Sedbergh School without the authority of Sedbergh School.

Internet and Email Conditions of Use
All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.

- Access, download, send or receive any data (including images), which Sedbergh School considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Sedbergh School, alter any information about it, or express any opinion about Sedbergh School, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward Sedbergh School mail to personal (non-Sedbergh School) email accounts (for example a personal Hotmail account).
- Make official commitments through the internet or email on behalf of Sedbergh School unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect Sedbergh School devices to the internet using non-standard connections.
- Store personal files such as music, video, photographs or games on Sedbergh School IT equipment.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, Sedbergh School has a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-Site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with Sedbergh School's remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.

- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN.

Mobile Storage Devices
Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Sedbergh School authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software
Employees must use only software that is authorised by Sedbergh School on Sedbergh School's computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on Sedbergh School computers must be approved and installed by the Sedbergh School IT department.

Viruses
The IT department has implemented centralised, automated virus detection and virus software updates within Sedbergh School. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:
- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Sedbergh School anti-virus software and procedures.

Telephony (Voice) Equipment Conditions of Use
- Use of Sedbergh School voice equipment is intended for business use. Individuals must not use Sedbergh School's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not:
- Use Sedbergh School's voice equipment for conducting private business.
- Make hoax or threatening calls to internal or external destinations
- Accept reverse charge calls from domestic or International operators, unless it is for business use.

Actions upon Termination of Contract
All Sedbergh School equipment and data, for example laptops and mobile devices, including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Sedbergh School at the end of your employment or termination of contract.

All Sedbergh School data or intellectual property developed or gained during the period of employment remains the property of Sedbergh School and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering
All data that is created and stored on Sedbergh School computers is the property of Sedbergh School and there is no official provision for individual data privacy, however wherever possible Sedbergh School will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Sedbergh School has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

This policy must be read in conjunction with Sedbergh School's Remote Working Policy

It is your responsibility to report suspected breaches of security policy without delay to the Deputy Bursar (Compliance), your Line Manager, or the IT Department.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Sedbergh School disciplinary procedures.