SEDBERGH SCHOOL

E-Safety Policy	
Version	2024.2
Effective from	October 2024
Extent of Policy	Sedbergh School Casterton, Sedbergh Preparatory School Sedbergh School Developments Ltd Sedbergh School International Ltd
Policy Owner	Senior Deputy Head (Pastoral)
Governor	John Campbell
Review by	September 2025
Frequency of Audit	Annual
Circulation	Staff Handbooks 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 IT Systems and Internet technologies.

1.3 The Designated Safeguarding Lead (DSL) and the Head of IT & Digital Strategy have responsibility for ensuring this policy is upheld by all members of the Sedbergh 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 to address any e-safety issues which may arise in classrooms on a daily basis.

1.4 Sedbergh School 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 on the School's CPOMS system as soon as possible if any incident relating to e-safety occurs and if necessary, directly to the DSL. Should a member of staff encounter anything that causes them concern on a pupil's account or personal device they should immediately notify the DSL and secure the device from any interference by others. Under no circumstances must they view, copy or forward the material concerned, 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 of misusing the IT system

2.1 The relevant IT Acceptable Use Policy applies to all users of Sedbergh School's IT systems.

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 defines potential abuse via the Internet. Please see: **Department for Education**

2.4 Pupils are aware of the consequences of misusing School IT systems these are laid out in the relevant Behaviour, Rewards & Sanctions Policies.

2.5 Staff need to be aware of the consequences of misusing School IT systems these are laid out in the Staff Code of Conduct.

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

4. Details of how the School builds resilience and develops pupils' understanding of e-safety

4.1 The PSHEE (CSPS) and Sedbergh Compass (Senior School) syllabus seeks to heighten awareness, understanding of and resilience to forms of threat found online.

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 use 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. Pupils are formally taught about online safety in age-appropriate 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 how to report their concerns and seek help if they encounter difficulties online.

Advice and support in such situations are 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. Pupils are signposted to the advice and support available through their PSHEE lessons and other opportunities in School.

5. Details 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 the School's 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 the network.

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 always observed.

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.

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/pin 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 are permitted to use personal devices.

6.2 **Pupils** – All pupils from Year 8 to Year 13 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.

No mobile phones or smart devices 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 these devices. Devices remain the responsibility of the child in case of loss or damage.

The functionality of smart devices is constantly evolving, for the purpose of this policy, a smart device is one that provides access to the Internet or the capability of communicating with others.

If devices are 'data-enabled', it is the parents' responsibility to enable mobile network-level age controls and monitor and control pupils' internet access and application downloads. Information on how to enable parental controls is available here:

https://www.internetmatters.org/parental-controls/broadband-mobile/

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

7. Use of Internet, e-mail and other digital services.

7.1 Network security systems allow the School to block websites or Internet services deemed inappropriate and identifies concerning communications, use, or content using School-provided services to connected devices. System reports are checked on a regular basis and the DSL or other appropriate member of staff is informed of concerns reported.

STAFF

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

7.4 Anti-virus and firewall protection is in place. Staff should be aware that communications sent via School provided services are monitored. Copies of all communications are retained for future reference should they be needed.

7.5 Staff must immediately report to the DSL, their line manager or the Head of IT & Digital Strategy any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should 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
    - post links or material which is discriminatory or offensive.
    - all written communications should be treated as being in the public domain.

7.7 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 carries 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.

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

PUPILS

7.9 All pupils are issued with their own School e-mail addresses. Access is via a personal login, which is password protected. This email service must be used for all School related matters. Pupils should be aware that communications using Sedbergh School's IT systems are monitored.

7.10 Anti-virus and firewall protection is in place. Certain websites are automatically blocked by the School's filtering systems. If this causes problems for School work/research purposes, pupils should contact their teacher for assistance.

7.11 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.

7.12 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.

8. Password Security

8.1 All users have individual School network logins and cloud-based storage folders. Staff and pupils are regularly reminded of the need for password security.

8.2 All users should:

- use a strong password containing eight characters or more, and contain a combination of upper and lower case letters as well as numbers; and
- change their passwords regularly (it is suggested at least termly).

Users must not:

- write passwords down or
- Allow anyone else to use their user ID/password on any Sedbergh School IT system, this includes access to the Wi-Fi.

9. Data storage

9.1 The School takes its compliance with the UK General Data Protection Regulations seriously. Please refer to the Privacy Notices on the School website and the IT Acceptable Use Policy (see appendix) for further details.

9.2 Staff and pupils are required to save all data relating to their work to either their School OneDrive, SharePoint or network folder.

9.3 If staff use personal devices for School work, they must be secured by password access controls. All data must be stored as outlined in 9.2.

Wherever possible, OneDrive or SharePoint should be used for the transfer or sharing of data. If it is unavoidable to use removeable media advice must be sought from the IT Department in advance.

Staff travelling abroad and who need to take any form of School data with them should contact the Bursar (Compliance) for advice as 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. They should recognise the risks attached to publishing their own images on the Internet (e.g. 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 be harmful or 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 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.

MLM
October 2024

Appendix I

ACCEPTABLE USE OF IT POLICY (All Staff & Senior School Pupils)

This Acceptable Use of IT Policy covers the security and use of Sedbergh School, Casterton, Sedbergh Preparatory School and its subsidiaries hereafter referred to as 'Sedbergh School', information, IT equipment, systems and services.

It also includes the use of email, Internet, voice and mobile IT equipment.

This policy applies to all Sedbergh School employees at both Schools, senior school pupils, 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.

Pupil Access to Mobile Phones

- Pupils in Years 9, 10 and 11 must hand their mobile phones in at published times for safe storage overnight with the HSM. This also applies to School trips.
- Pupils in Years 12 and 13 are permitted to keep their mobile phones overnight.
- Access to mobile phones can be withdrawn at any time at the discretion of HSMs if behaviour or use of electronic devices has been unsatisfactory or of concern.
- Full details of pupils' permitted access to mobile phones, as well as School Rules on the appropriate use of mobile phones, may be found in the Brown Book.

Computer Access Control – Individual's Responsibility

Access to the Sedbergh School IT systems is controlled via 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 Sedbergh School's IT systems.

Individuals must not:

- Allow anyone else to use their user ID/password on any Sedbergh School IT system, this includes access to the Wi-Fi.
- 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 and narratives on the Internet and email systems.

Individuals must not:
- Use the Internet, email or other digital services 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, email or other digital services to make personal gains or conduct a personal business.
- Use the Internet, email or other digital services to gamble.
- Use the Internet, email or other digital services 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 data to personal (non-Sedbergh School) email accounts (for example a personal Gmail account).
- Make official commitments through the Internet, email or other digital services on behalf of Sedbergh School unless authorised to do so.
- Download copyrighted material such as music media files, film and video files without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Remove or disable anti-virus software.
- Download or subscribe to any software from the Internet, email or other digital services without prior approval of the IT Department.
- Connect Sedbergh School devices to the Internet using non-standard connections.

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 School provided laptops and mobile devices may be taken off-site. The following controls must be applied:

- School provided equipment and media taken off-site must not be left unattended in public places.
- Devices 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).
- 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 & Subscriptions
Employees must only use software or subscribe to services authorised by Sedbergh School following approval by the School's IT Department and completion of a Data Protection Impact Assessment (DPIA). Software and subscriptions must be used in accordance with the supplier's licensing agreements.

IT Equipment
Individuals provided with any equipment or devices such as laptops, tablets and mobile phones are required to ensure it is kept in good condition and that any loss or damage is reported immediately to the IT Department. If protective devices are provided by Sedbergh School this must be used alongside any Sedbergh School provided equipment.

Should an insurance claim be made for any loss or damage to Sedbergh School provided equipment individuals may be asked to contribute to an insurance excess.

Individuals must return Sedbergh School provided equipment at the request of the IT Department or their Line Manager.

Use of Sedbergh School provided equipment is subject to individuals using such equipment whilst undertaking their duties at Sedbergh School. Upon completion, contract termination, change in duties or request by the School, Sedbergh School provided equipment must be promptly returned to the IT Department where all data held on the equipment will be removed.

Telephony Equipment, Conditions of Use
Use of Sedbergh School provided telephony equipment is intended for business use. Individuals must not use the equipment for sending or receiving private communications on personal matters, except in exceptional circumstances.

Individuals must not:
- Use Sedbergh School provided telephony 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 leaving Sedbergh School
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 or when leaving the School.

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 departure or reused for any other purpose.

Monitoring and Filtering
All data created and stored on School provided devices or systems remains the property of the School.

Where reasonable suspicion exists of a data breach or a breach of this, or any other policy, the School has the right to monitor activity on its systems, including the Internet and email use. This is to ensure systems are secure, effective in operation and to protect against any possible misuse.

Any monitoring of our systems, or of individual user accounts, will be completed in accordance with the UK Data Protection Act 2018, the Regulation of Investigatory Powers act 2000 and the Communications (lawful business practice, interception of communications) Regulations, our own Privacy Notices, and any other of the School's relevant internal policies.

It is your responsibility to report suspected breaches of this policy, without delay, to your Line Manager, Housemaster or Housemistress or the IT Department

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

Please click here to confirm that you have read, understood and accept the ACCEPTABLE USE OF IT POLICY.

Appendix II

ACCEPTABLE USE OF IT POLICY (CSPS Pupils)

1. Overview

The essence of the code is respect for other users and, integral to this, respect for the system and equipment. You should not do anything that is offensive, damaging to other users or their work, damaging to the system, or illegal. The rules and guidelines in this document must be adhered to. The School reserves the right to withdraw network and/or Internet access from pupils who fail to respect the Acceptable Use of IT Policy (CSPS Pupils).

2. Use of the School Network

Pupils agree to:

- keep their passwords secret.
- look after the equipment they use.
- only use the computers for the tasks authorised by a member of staff.
- ask permission from the IT department before physically connecting or disconnecting any device or accessory to or from the network or other School computing equipment.
- ask permission from the IT department before copying, installing or downloading any programs on any School-owned equipment.

Pupils will not:

- access or attempt to access another user's files.
- attempt to bypass School filtering systems.
- use anyone else's log-on name.
- use the School network for online games.
- create messages or documents that appear to originate from someone else.
- create/publish or send any document/file that may be considered abusive, of a bullying nature, cause distress or otherwise be a nuisance.
- try to configure or change any settings on the School computers, other than those to which pupils are granted access.
- attempt to bypass, hack or defeat any School computer or server or in any way tamper with network security.
- connect any unauthorised equipment to the network.
- leave their computers logged on and unattended.
- look for, share or view any pornographic material.
- Download copyrighted material such as music media files, film and video files without appropriate approval.
- arrange meetings with strangers on any chat or social networking sites.
- enter an ICT suite until a member of staff is present.
- take food or drink into IT suites or near any computer equipment.

3. Internet and E-mail

Use of the Internet is a privilege, not a right. In the event of abuse, access will be removed. Pupils are provided with a School email account; use of web-based mail (Gmail/Hotmail/Yahoo etc) is not allowed.

4. Pupil Devices

Pupils are not permitted to carry mobile phones, smart device or tablets in School during the day. The functionality of smart devices is constantly evolving, for the purpose of this policy, a smart device is one that provides access to the Internet or the capability of communicating with others.

Pupils' devices must not include inappropriate applications. This applies to all pupils, whether over the age of 13 or otherwise.

Devices provided to boarders must have parental controls enabled which prevents pupils from downloading applications and accessing websites beyond their age rating. If devices are 'data-enabled', it is the parents' responsibility to enable mobile network-level age controls and monitor and control pupils' internet access and application downloads. Information on how to enable parental controls is available here:

https://www.internetmatters.org/parental-controls/broadband-mobile/

- Pupils who come on the School bus may require a mobile phone to contact parents regarding collection. In making this decision, parents should note that all bus drivers will also have a record of contact numbers.
  - All pupils bringing a phone onto a regular School bus MUST have the permission of their parent to do so and will be added to the Mobile Device Register.
  - The phone or tablet must be handed to the School Office immediately upon arrival and collected at the end of the day.
  - It should not be used in School at all.
  - Where a pupil on a School bus is listed on the Mobile Device Register and is in School, we would expect a device to be in the Main Office or an explanation provided if it were not.
- Pupils on School trips, including travel to sports fixtures, are not permitted to bring a device on trips unless overnight. In which case, the devices will be collected by staff and provided in the evenings for a fixed time before collection again overnight.
- Weekly and Flexi-boarders arriving in the morning may bring in phones or tablets to use at designated times in the evenings. On the morning they arrive, the device should be handed to either the houseparent or matron or their boarding house. If neither is available, they can be handed to the Main Office instead.
- Pupils on residential trips and tours will be subject to the same controls as above. Staff will issue any phones for a controlled period in the evening and then collect overnight.
- Pupils are in no way to engage in cyber bullying using any device.

Failure to follow this guidance will result in the privilege being withdrawn and confiscation of the device.

5. IT Management

- Users accept that their time spent on the School network is monitored by the School, either directly, remotely, or both. This is to ensure the safety of users and that the network is being used for the intended purpose.
- Use of the network and Internet is monitored.

- In exceptional circumstances, e-mails may be read on the instructions of the Head, the Deputies, the DSL, the Head of IT & Digital Strategy or the pupil's Housemaster/ Housemistress.

7. Sanctions

Possible punishments, depending on the severity and frequency of the offence, include:

- Varying periods of denial of access to either Internet, e-mail or the School network.
- Confiscation of equipment.
- Standard School punishments, including detention, suspension and exclusion.

8. Microsoft Teams

It is essential that you not only know how to use Microsoft Teams, but you also know how to use it safely and responsibly.

- Microsoft Teams is an extension of the School and you must behave accordingly. All interactions with pupils (including social), and staff should be polite and courteous.
- I will complete and upload all prep into Teams by the deadlines directed by the teacher.
- I will not record or take photos of my classmates or teachers during online sessions.
- I understand that when using Microsoft Teams and other applications provided by the School that my use can be monitored and details can be made available to my teachers.

9. Monitoring and Filtering

All data created and stored on School provided devices or systems remains the property of the School.

Where reasonable suspicion exists of a data breach or a breach of this, or any other policy, the School has the right to monitor activity on its systems, including the Internet and email use. This is to ensure systems are secure, effective in operation and to protect against any possible misuse.

Any monitoring of our systems, or of individual user accounts, will be completed in accordance with the UK Data Protection Act 2018, the Regulation of Investigatory Powers act 2000 and the Communications (lawful business practice, interception of communications) Regulations, our own Privacy Notices, and any other of the School's relevant internal policies.

It is your responsibility to report suspected breaches of this policy, without delay, to your Housemaster / Housemistress

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

Please click here to confirm that you have read, understood and accept the ACCEPTABLE USE OF IT POLICY.