SEDBERGH SCHOOL

E-Safety Policy

Version	2016.2
Effective from	July 2016
Extent of Policy	Sedbergh Senior School
Policy Owner	Colin Gunning
Governor	Tbc
Review by	July 2017
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 **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 IT Manager 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. We regularly remind parents/guardians about e-safety issues and seek to promote a wide understanding of the benefits and risks related to internet usage.

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** 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 2015 defines potential abuse via the internet. Please see: **KCSIE 2015**.

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 PSHEE 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). Karl Hopwood is the most regular guest speaker.

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 recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils can report concerns to any member of staff at the School. The CEOP link is permanently present on the School's desktop

4.6 Teaching Children to Stay Safe

Pupils will often have access to technologies that have both positive and negative potential. Consideration should be given to the use of technology within the School setting and beyond, with a policy that is clear, understood and respected by staff, pupils and the wider School community. Whilst each school's perspective and practice will vary, the policy should ensure the school's expectations and safeguarding obligations are communicated and effective. A policy should include guidance on:

(a) Clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with other safeguarding policy;

(b) Clear guidance on the use of technology in the classroom and beyond for all users, including staff, students/pupils and visitors that references permissions/restrictions and agreed sanctions;

(c) Detail the school's technical provision/infrastructure and the safeguards in place to filter and monitor inappropriate content and alert the school to safeguarding issues;

(d) Detail on how the school builds resilience in its students to protect themselves and their peers through education and information;

(e) Detail on staff safeguarding professional development that includes online safety;

(f) Reporting mechanisms available for all users to report issues and concerns to the school and how they are managed and/or escalated;

(g) How the school informs, communicates with and educates parents/carers in online safety;

(h) The management of personal data in line with statutory requirements.

5 Detail on staff Safeguarding professional development that includes online safety

5.1 Safeguarding Policy 2016

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** 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** **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 SLT 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.

9 Data Storage

9.1 The School takes its compliance with the Data Protection Act 1998 seriously. Please refer to the **Data Protection Policy** 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 either onto a School laptop or to the School's central server.

9.3 If staff use personal devices they should be encrypted if any pupil data or School passwords are stored on them. The School expects all removable media USB memory sticks, CDs, portable drives containing pupil data which are being sent by post or courier to be encrypted before sending. Staff may only take information offsite when it is necessary and required in order to fulfil their role.

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** 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**.

SRA/CH
May 2016