Selby
Educational Trust

Title	Reviewers	Reviewed and Approved		Review Date
e-Safety Policy	Ian Clennan & Mike Pilling	Trust Meeting	May 2023	May 2024

To be reviewed every year

E-SAFETY POLICY

1 Introduction

Selby Educational Trust recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the Trust while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In our duty to safeguard learners, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care.

This e-safety policy should be read alongside other relevant Trust policies eg Safeguarding.

2 Purpose and Policy Statement

The purpose of this policy is to guide staff and learners to the safe use of Trust and school IT systems and Internet both at school and off site.

The 4 key categories of risk
Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

3 Definition: what is an e-Safety Policy?

An e-Safety policy helps to promote use of technology to enhance learning within the Trust and to ensure learners get the most from it, by encouraging responsible online behaviour. An e-safety policy helps minimise risk and embed important principles such as:

- keep personal information private
- consider the implications of any content posted online
- do not upload or post inappropriate, offensive or illegal content to their own or other online spaces.

4 Scope

This policy applies to all learners, staff or others who have access to the Trust IT systems, both on the premises and remotely. Any user of the Trusts IT systems must adhere to the Computer Network and Usage Policy and the Pupil Computer and Network User Policy.

The e-Safety Policy applies to all use of the internet and electronic communication devices such as e-mail, mobile devices, social networking sites, and any other systems that use the internet for connection and providing of information.

The policy also takes into account the National Curriculum computing programmes of study.
This policy complies with our funding agreement and articles of association.

5 Responsibilities

The Trust has a responsibility to:

- Ensure Trust resources are used responsibly and safely by learners and staff.

All managers are responsible for:

- Ensuring their staff are aware of this policy and procedure and how it operates.

The designated safeguarding lead:

Details of the school’s designated safeguarding lead (DSL) [and deputy/deputies] are set out in our child protection and safeguarding policy as well as relevant job descriptions.
The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

Individual members of staff have a responsibility to:

- Be aware of this policy and procedure and how it operates.

- Ensure the safety of pupils
- MUST report any concerns or disclosures immediately to a Designated Safeguarding Lead (DSL)
- NEVER offer assurance of confidentiality everything discussed MUST be reported
- Keep to the terms and conditions of the IT Acceptable Use Policy at all times
- Attend staff training on e-safety and display a model example to pupils at all times
- Actively promote through embedded good e-safety practice.

Individual pupils have a responsibility to:

- Use Trust resources and the Internet in a responsible and safe manner and in the event of any e-Safety concerns to contact the Headteacher in the first instance,

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
- Parents can seek further guidance on keeping children safe online from the following organisations and websites: What are the issues? – UK Safer Internet Centre Hot topics – Childnet International Parent resource sheet – Childnet International

6.1 Technologies

The technologies covered by this policy are computer, Internet, electronic communication and mobile devices such as mobile/smart phones and PDAs.

Current Internet technologies used both inside and outside of the classroom include:

- Websites
- Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video and Music Downloading.

6.1 Staff Using Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates
- Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.
- Work devices must be used solely for work activities.

- If staff have any concerns over the security of their device, they must seek advice from [relevant role of individual, e.g. the ICT manager].

7 Stakeholders

This means that designing and implementing e-safety policies demands the involvement of a wide range of interest groups:

- CEO and school Headteachers
- Trustees
- Governors
- Senior Managers
- Teachers and Support Staff
- All pupils, particularly young people and vulnerable adults

8 Creating a Safe ICT Learning Environment

The Trust has implemented systems to minimise the risk of accessing inappropriate & unacceptable information, applications, websites etc. these are:

- Firewalls, to stop unwanted intrusion from external locations and ensure that students/staff cannot access external websites without using the Internet content filtering system
- Internet content filtering, this categorises web site content and by the use of rules either allows/disallows access to websites
- Virus protection, checks all files, emails, websites for virus and cleans/quarantines the virus as appropriate
- Network security, through the use of the usernames and passwords students and staff can only access their own files or designated shared access areas
- Group policy, restricts the ability of students and staff when using SET computers to install software and make changes to the computer systems.
- Selby College IT systems and the College's Information Security Management System is certified to meet the following Information Security and Cyber Security standards- Cyber Essentials Scheme

9 Monitoring

The use of IT may be monitored in school. This includes the logging on/off of computers systems, Internet activity, Virtual Learning Environment , and e-mails. Monitoring will only be used to confirm or investigate compliance with SET policies and procedures. Staff are advised not to read personal e mails on Trust and school computers.

10 Internet Use

It is impossible to be completely protected while using the internet. However, you can take simple steps to reduce the risks as outlined below.

10.1 Search Engines Sites

Search engines enable the rapid search of the Internet for information, whether this information is text, image or sound. Searching consists of entering a word or words into a search box and clicking the search button, which sets in motion a search engine that automatically produces a list of the addresses of websites relevant to the words entered.

Many search providers also offer the facility for the user to search for images, video and audio content.

The more accurate your search is (ie using more than one relevant word), the more relevant the search results will be and thus the less likely that unwanted results will be prominently returned. For example, if you are searching for information on the planet Mercury, entering ‘planet mercury’ into the search box will get more relevant results than just entering ‘Mercury’.

Take care to spell correctly when typing in a search. Even a small typing error can bring up unwanted results.

Remember that not all the information in websites returned in searches is reliable. There are things you can do to assess the quality of the information you find (see www.quick.org.uk for example).

There are two types of search results (see above for more information on this):

- Automated search results and
- Sponsored listings

Search providers usually separate and label these but it is important that you are aware of the difference and can differentiate them in the results of the search provider you are using.

Whichever search provider you choose, it is important that you familiarise yourself with this provider’s service, finding out about the search provider’s safety advice, the search provider’s filter, how to contact the search provider, and how sponsored listings are differentiated from other search results.

10.2 Social Networking Sites

Social networking sites (like Facebook, MySpace or Twitter) are online ‘communities’ of internet users with similar interests. Members of the community create an online ‘profile’ which provides other users with varying amounts of personal information.
Once users have joined the network, they can communicate with each other and share things like music, photos and films. The sites are a fun way to stay connected with friends, family and peers.

As with most potential online dangers, the problems can start if you do not look after personal information properly. The risks you need to be aware of are:

- Cyberbullying (bullying using digital technology)
- Invasion of privacy
- Identity theft
- Seeing offensive images and messages
- The presence of strangers who may be there to ‘groom’ other members.

10.3 Staying Safe Using Social Networking Websites:

- Don’t publish personal information like location, email address, phone number or date of birth
- Be very careful about what images and messages are posted, even among trusted friends - once they are online they can be shared widely and are extremely difficult to get removed

- Keep a record of anything abusive or offensive received and report any trouble to the site management (most sites have a simple reporting procedure, normally activated by clicking on a link on the page)
- Be aware that publishing or sharing anything which would mean breaking a copyright agreement is illegal
- If you make an online friend and want to meet up with them in real life, ensure you have a responsible adult with you to check the person is who they say they are
- Be aware of online scams - offers which seem too good to be true usually are
- Do not to get into any online discussions about sex as this tends to attract potentially dangerous users.
- Ensure your privacy settings are correctly set.

10.4 E-mail

- Do not forward chain letters to anyone else, just delete them
- Do not impersonate anyone else using e-mail
- Do not use e-mail to send comments or information that is defamatory or libellous, or use e-mail as a means of harassment, intimidation, annoyance or bullying to anyone else. The sender of an e-mail should only send messages the contents of which they would be happy to receive or have read out in court. E-mail messages are admissible as evidence
- Do not reply to pestering, offensive or suggestive e-mails, students should report such occurrences to a teacher or IT Services
- The biggest cause of computer viruses is sent by email, often innocently. If you think you have received a virus, or are suspicious about an email received, delete the email without opening it and report it to IT Services.

11 E-Safety Concerns and Complaints

The Trust will not tolerate any abuse of ICT systems or associated technologies. Whether offline or online, communications by staff and students should be courteous and respectful at all times. Any reported incident or bullying - including cyber bullying, harassment or other unacceptable behaviour will be treated seriously.

Where conduct is found to be unacceptable, the Trust will deal with this internally. Where conduct is considered illegal, the matter will be referred to the Police. Additionally, the Trust may seek to involve other agencies where conduct is believed to be unacceptable or illegal.

Concerns relating to safeguarding, including child protection must be must be referred immediately to the designated person responsible for safeguarding/child protection.

12 Curriculum

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

13 **Behaviour**

Use of any Selby Educational Trust's IT equipment and systems is conditional to the Trust Policies including the IT Acceptable Use Policy & the Anti-Bullying Harassment Policy and Procedure. Communications by staff and pupils should be courteous and respectful at all times whether offline or online. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the Anti-Bullying and Harassment Policy (staff and pupils).

Cyber Bullying Cyber bullying is a form of bullying. As it takes place online, it is not confined to Selby Educational Trust buildings or school hours. Cyber bullies can communicate their messages to a wide audience with speed and often remain anonymous or unidentifiable. Cyber bullying includes bullying via:

- Text message and messaging apps e.g. sending unwelcome texts or messages that are threatening or cause discomfort.
- Picture/video-clips e.g. using mobile device cameras to bully someone, with images usually sent to other people or websites.
- Phone call e.g. silent calls or abusive messages. The bully often disguises their number.
- Email e.g. emailing upsetting messages, often using a different name for anonymity or using someone else's name to pin the blame on them.
- Chat room e.g. sending upsetting responses to people when they are in a web-based chat room.
- Instant Messaging (IM) e.g. sending unpleasant messages in real-time conversations on the internet.
- Websites e.g. insulting blogs, personal websites, social networking sites and online personal polling sites.

Where conduct is found to be unacceptable, the Selby Educational Trust will deal with the matter internally and refer to relevant policies, for example, the Disciplinary Policy. Where conduct is considered illegal, Selby Educational Trust will report the matter to the police.

13 Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
All trustees and governors will undertake online training after appointment. Certificates will be shared.
By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
Children can abuse their peers online through:
o Abusive, harassing, and misogynistic messages
o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
o Sharing of abusive images and pornography, to those who don't want to receive such content
Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL [and deputy/deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

15 Equality and Diversity Statement

Selby Educational Trust welcomes and celebrates equality and diversity. We believe that everyone should be treated equally and fairly regardless of their age, disability, gender, gender identity, race, religion or belief, sexual orientation and socio-economic background. We seek to ensure that no member of the Trust community receives less favourable treatment on any of these grounds which cannot be shown to be justified.

This document is written with the above commitment, to ensure equality and diversity is at the centre of working life at Selby Educational Trust.

16 Safeguarding & Prevent Policy

Selby Educational Trust recognises its moral and statutory responsibility to safeguard and promote the welfare of students. We work to provide a safe and welcoming environment where students are respected and valued. We are alert to the signs of abuse, neglect, radicalisation and extremism and follow our procedures to ensure our students receive effective support, protection and justice. Selby Educational Trust expects governors, staff and volunteers working on behalf of the Trust to share this commitment.

The following guidance must be adhered to by all staff communicating online:

- Staff must not post any personal views, beliefs or opinions
- Staff must challenge any personal views, beliefs or opinions posted by pupils

- Staff must post with counter arguments to any personal view, beliefs or opinions posted by learners which undermine British Values
- Any post considered to isolate or put a young person or vulnerable adult at risk should be referred to a Safeguarding Officer for further investigation
- Any post considered to promote extreme views should be referred to a Safeguarding Officer for further investigation

17 Fraud, Bribery & Corruption

Selby Educational Trust follows good business practice and has robust controls in place to prevent fraud, corruption and bribery. Due consideration has been given to the Fraud Act 2006 and the Bribery Act 2010 in the development/review of this policy document and no specific risks were identified.

18 Useful Links

- Childnet's Professional resources: http://www.childnet.com/teachers-and-professionals
- NCA-CEOP Ambassador course: https://www.thinkuknow.co.uk/professionals/training/ceop-ambassador-course/
- NSPCC and NCA-CEOP - Keeping Children Safe Online. an online introductory safeguarding course for anyone who works with children (2019 version): https://www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-childrensafe-online-course/
- UK Safer Internet Centre training, advice and resources for teachers and professionals: https://www.saferinternet.org.uk/advice-centre/teachers-and-schoolstaff and Online Safety Briefings: https://www.saferinternet.org.uk/training-events/online-safety-live-free-online-safetyevents
- Access any local support available - some local authorities, local safeguarding partners and/or regional broadband consortia offer online safety training for professionals
- DfE 'Teaching Online Safety in Schools' guidance https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- DfE Statutory (September 2020) guidance for Relationships Education, Relationships and Sex Education (RSE) and Health Education https://www.gov.uk/government/publications/relationships-education-relationshipsand-sex-education-rse-and-health-education
- NCA-CEOP's online safety education programme, Thinkuknow: http://www.thinkuknow.co.uk
- PSHE Association/NPCC using police in the classroom guidance https://www.pshe-association.org.uk/policing
- UKCIS 'Education for a Connected World' framework: https://www.gov.uk/government/publications/education-for-a-connected-world
- UKCIS 'Using External Visitors to Support Online Safety Education: Guidance for Educational Settings' https://www.gov.uk/government/publications/using-external-visitors-to-supportonline-safety-education-guidance-for-educational-settings