SILCOATES

E-Safety, Social & Digital Media Policy

E-Safety, Social and Digital Media Policy

Silcoates School (the School) recognises that technology and the internet are excellent tools for learning and communication that can be used in school to enhance the curriculum, challenge pupils, and support creativity and independence. Using technology to interact socially and share ideas can benefit everyone in the School community. However, it is important that the use of the internet and technology is seen as a responsibility and that pupils, staff and parents use it appropriately and practise good e-safety. It is important that all members of the School community are aware of the dangers of using the internet and how they should conduct themselves online.

E-safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children to help in the educating all members of the school community on the risks and responsibilities of e-safety. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating technology activity in school, and provide a good understanding of appropriate use that members of the school community can use as a reference for their conduct online outside of school hours.

E-Safety is a whole-school community issue and responsibility.

Cyberbullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures which are outlined in our Anti-Bullying Policy.

Roles and responsibility

The designated member of the SLT responsible for E-Safety is the Deputy Head (Pastoral).

Filtering and Monitoring

In order to keep pupils safe online the School uses filters to block access to harmful content. Sophos Firewall is used to filter content for any pupils using their own device on the network and on School PCs. If pupils require access to a blocked site for academic reasons, they can request access by reporting the site to the Network Manager. The School also monitors pupil use of ICT. Net Support DNA is used to monitor School based PCs and Senso is used to monitor activity on Chromebooks (including when used off-site). Alerts are sent to the DSL when pupils try to access concerning material who is able to investigate further.

Mr Chris Evans is the person responsible for filtering and monitoring systems. Mrs Barbara Tibbets is the Governor responsible for filtering and monitoring. All teaching staff are responsible for monitoring pupil ICT use in lessons and receive training on how to do so.

The effectiveness of filtering and monitoring within the School will be evaluated by the DSL, Systems Manager and Safeguarding Governor formally each April. However, the DSL and Systems Manager will continue to review the systems on an ongoing basis.

Communicating school policy

This policy is available on the School's website. Rules relating to the School's code of conduct when online, and e-safety guidelines, are displayed around the school. E-Safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and Personal Development lessons where personal safety, responsibility, and/or development are being discussed. It is also a part of the Sixth Form induction process and Assembly content.

Making use of technology and the internet in school

The internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our pupils with all the necessary skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Learning to evaluate internet content

With so much information available online it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the School as part of digital literacy (supported by the ICT curriculum) across all subjects. It is also supported by the curriculum's core themes of research, questioning and communication. The School will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported to the IT Support Department. Any material found by members of the School community that is believed to be unlawful will be reported to the appropriate authorities and/or agencies. Regular software and broadband (WiFi) checks will take place to ensure filtering services are working effectively.

Managing information systems

The School is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal information of our School community extremely seriously. Steps are taken to protect the

School network, as far as is practicably possible, against virus infection, hackers and other external security threats. The security of the School information systems will be reviewed on a regular basis by the Network Manager, and firewall protection software updated regularly. Some safeguards that the school takes to secure our computer systems are:

- ensuring that all personal data sent over the internet or taken off site is encrypted
- making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- files held on the School network will be regularly checked for viruses
- the use of user logins and passwords to access the School network will be enforced with additional authentication methods used to enhance security
- portable media containing school data or programmes must be kept securely at all times.

For more information on data protection in school please refer to our **Privacy Policy/Notice** on the School website.

Emails

The School uses email internally for staff and pupils, and externally for contacting parents. Email is an essential part of school communication and is also used to enhance the curriculum by:

- providing contact with pupils regarding upcoming dates/events/notices;
- providing immediate feedback on work, and requests for support where required.

Staff and pupils should be aware that school email accounts should only be used for school-related matters. This is important for confidentiality. The School has the right to monitor emails and their contents.

Staff, parents and pupils should communicate, wherever possible, using school email addresses and should not exchange personal email addresses.

Published content and the School website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, pupils, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the School community, copyrights and privacy policies. No personal information on staff or pupils will be published; only school email addresses and telephone numbers are published.

Policy and guidance of safe use of children's photographs and work

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

The School's Taking, Storing and Using Images of Children Policy, alongside the School's Privacy Policy/Notice (both available on the School website) explains the School's approach, responsibilities and processing of such information and data.

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place. It is important that published images do not identify pupils or put them at risk of being identified. Only images created by or for the School will be used in public and children may not be approached or photographed while in school or doing school activities without the School's permission.

The School follows general rules on the use of photographs of individual children:

Parental (or pupil) consent must be obtained.

Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (e.g., a pupil in a swimming pool, rather than standing by the side in a swimsuit).

Complaints of misuse of photographs or video

Parents should follow the standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our Complaints Policy for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the School's Safeguarding and Child Protection Policy.

Social networking, social media and personal publishing (including printed material)

Personal publishing tools include blogs, microblogs (Twitter), wikis, social networking sites (Facebook), bulletin boards, chat rooms and instant messaging programmes, content sharing sites (Tik Tok, Instagram, YouTube) and any such printed material. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. There are various restrictions on the use of these sites in school that apply to both pupils and staff.

Social media sites have many benefits for both personal use and professional learning; however, both staff and pupils should be aware of how they present themselves online. Pupils are taught through the ICT Curriculum and Personal Development about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The School follows general rules on the use of social media and social networking sites in school. These rules also apply to any printed material, such as departmental magazines/publications:

• Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are made fully aware of the School's code of conduct regarding the use of ICT and technologies and behaviour online.

• Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

• Official school blogs/social media accounts created by staff or pupils/year groups/school clubs as part of the School curriculum will be password-protected and run from the School website with the approval of a member of staff and will be moderated by a member of staff.

• Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The School expects all staff and pupils to remember that they are representing the School at all times and must act appropriately.

• Safe and professional behaviour of staff online will be discussed at staff induction and Inset, and governed by the Staff Code of Conduct.

Mobile phones and personal devices

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

• they can make pupils and staff more vulnerable to cyberbullying;

• they can be used to access inappropriate internet material;

• they can be a distraction in the classroom;

• they are valuable items that could be stolen, damaged, or lost;

• they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school takes certain measures to ensure that mobile phones are used responsibly in school. Some of these are outlined below.

• The school has in place a mobile phone policy which states that mobile phones should not be used during the school day without the express permission of a teacher.

• The school will not tolerate cyberbullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions read the School's Behaviour, Rewards and Sanctions Policy.

• Mobile phones can be confiscated by a member of staff, and the device can be searched by a member of the senior leadership team if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.

• Any pupil who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The School will not take responsibility for personal devices that have been lost, stolen, or damaged.

• Images or files should not be sent between mobile phones in school.

Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the Anti-Bullying Policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the School community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action. If an allegation of bullying does come up, the School will:

• take it seriously;

• act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully

• record and report the incident;

• provide support and reassurance to the victim;

• make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'perpetrator' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school.

Repeated bullying may result in a fixed-term or permanent exclusion.

Extremism and Radicalisation

Through its monitoring, if School becomes concerned about any pupil being at risk of being radicalised it has a duty to refer the matter to local Prevent staff, the Police or other services within the local authority.

Managing emerging technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk assess any new technologies before they are allowed or deployed in school, and will consider any educational benefits that they might have. The School keeps up-to-date with new technologies and is prepared to develop quickly appropriate strategies for dealing with new technological developments.

Protecting personal data

Silcoates School believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The School collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs.

Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and pupils.

For more information on the School's safeguards relating to data privacy please read the school's Privacy Policy/Notice (available on the School website).

Notes for staff:

Benefits of technology and internet in schools

• Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.

• Immediate professional and personal support through networks and associations.

• Improved access to technical support.

• Ability to provide immediate feedback to pupils and parents.

• Class management, attendance records, schedule, and assignment tracking.

Appropriate email use in school

Staff should be aware of the following when using email in school:

• Staff should only use official school-provided email accounts to communicate with pupils, parents or carers. Staff should not send emails to multiple email addresses, and take measures to protect unauthorised sharing of personal information with wider groups of individuals.

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

• Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

• The forwarding of chain messages is not permitted in school.

Mobile phone or personal device misuse

• Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of school time.

• Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the School equipment will be used for this.

• The School expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours. If staff need to use their phone, it should be in an office, or in the Common Room, out of sight of pupils.

• Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the Staff Handbook.

Official school social media accounts, websites and publications

• Prior to creating a social media account, or website, or publication careful consideration must be given to the purposes for using such medium and whether the overall investment is likely to be worthwhile for achieving the proposed pedagogical outcome.

• The proposed audience and level of interactive engagement with the site, (eg whether pupils will be able to contribute content to the site) must be considered.

• Staff members must consider how much time and effort they are willing to commit to the proposed site. They should be aware that maintaining a social media account or website is not a one-off task, but involves a considerable time commitment, particularly in terms of updating and checking the validity of friends/followers.

• It is important that enough staff members are trained and are able to maintain and moderate an account/website in case of staff absences or turnover.

• There must be a careful exit strategy and a clear plan from the outset about how long the account/website will last. It must not be neglected, creating a potential risk to the School's brand and image.

• Consideration must also be given to how the success of the account/website will be evaluated to assess whether it has achieved the proposed objectives.

Approval for the creation of social media accounts, websites and publications

• Staff must complete the Social Media/Website/Publication Creation Approval Form **(Appendix A)** and forward it to the Marketing Co-ordinator before creation.

• Silcoates School social media accounts/websites can be created only by or on behalf of the School.

• The Marketing Manager must be consulted about the purpose of the proposed account/website and its content.

• The Marketing Manager's approval must be obtained for the use of the School logo and brand.

• The Marketing Manager reserves the right to monitor the quality and content of school social media accounts, websites and publications.

• A social media site may attract media attention. All media enquiries should be directed to the Marketing Manager or Head immediately. Staff members should not communicate with the media without advice and approval.

• Final approval regarding the creation of a social media account, website, or publication remains with The Head.

Content

• Information provided must be worthwhile and accurate; remember what is published will reflect on the School's image and reputation.

• Content must stay within the law and be aware that child protection, privacy, data protection, libel, defamation, harassment and copyright law may apply to the content of social media.

• Permission must be sought from the relevant people before citing or referencing their work or referencing service providers, partners or other agencies.

• Social media sites must respect their audience and be sensitive in the tone of language used and when discussing topics that others may find controversial or objectionable.

• Silcoates School hosted sites must always include the School logo or brand to ensure transparency and confidence in the site.

Notes for pupils:

Benefits of ICT and internet in schools

• Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.

• Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.

• Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.

• An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.

• Access to learning whenever and wherever convenient.

• Freedom to be creative.

• Freedom to explore the world and its cultures from within a classroom.

• Social inclusion, in class and online.

• Access to case studies, videos and interactive media to enhance understanding.

• Individualised access to learning.

Evaluating internet content pupils will be taught:

• to be critically aware of materials they read, and shown how to validate information before accepting it as accurate

• to use age-appropriate tools to search for information online

• to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the School will take any intentional acts of plagiary very seriously. Pupils who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

Appropriate email use in school

Pupils should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT Curriculum and in any instance where email is being used within the curriculum or in class:

• in school, pupils should only use school-approved email accounts to communicate with staff

• Pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

• Pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.

Pupils will be educated through ICT curriculum lessons to identify spam, phishing and virus emails and attachments that could cause harm to the School network or their personal account or wellbeing.

Mobile phone or personal device misuse

• Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's Behaviour, Rewards and Sanctions and Policy. Their mobile phone will be confiscated in line with the mobile phone policy.

• Pupils are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a pupil is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the pupil being prohibited from taking that exam.

Reviewed by:	Mr Lee – Interim Bursar Mr Evans – Deputy Head (Pastoral)		
Date of last review:	January 2024	Date of next review:	April 2024

APPENDIX A

Approval Form: Social/Digital media creation

Details:

Staff Name:	……………………………………….

Department:	……………………………………….

Purpose of site publication:

Aims:

Suggested (example) content:

Administration of site/account:

Host:	…………………………………………

Go-live date:	…………………………………………

Security measures:

Approval:

Marketing Dept:

Name:	……………………………………….

Signature:	……………………………………….

Date:	……………………………………….