ST HELEN &
ST KATHARINE

-

LENT 2021

SAFEGUARDING - ONLINE SAFETY POLICY

St Helen and St Katharine places safeguarding at the heart of all that we do; we recognise the wide-ranging aspects of the term.

There are three policies that comprise the Safeguarding Group - Child Protection, Prevent and Online Safety. This policy focuses on safeguarding in terms of online safety.

The Safeguarding Policy Group has alongside it a range of other important policies that work together to safeguard the individuals at this school. These policies are:

Whistleblowing, Anti-bullying, ICT Acceptable use, Equal Opportunities, Safer Recruitment, Sex and relationships, Health and Safety, Pastoral Care, Behaviour, Work Experience and the Staff Code of Conduct.

In writing the Safeguarding policies we have referred to: Keeping Children Safe in Education (September 2019) (KCSIE); Disqualification under the Childcare Act 2006 (September 2018) What to do if you're worried a child is being abused (March 2015) Working Together to Safeguard Children (2018); Revised Prevent Duty Guidance: for England and Wales (April 2019) (Prevent). The Prevent duty: Departmental advice for schools and childminders (June 2015); The use of social media for on-line radicalisation (July 2015). (These documents refer to the Children's Act 1989) UK Safer Internet Centre: appropriate filtering and monitoring.

AIMS

The aims of this policy and its supporting policies (see Use of Technology) are to:

- Set out the key principles expected of all members of the School community with respect to the use of digital technologies.
- Safeguard, protect and educate students and staff.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use for the whole school community.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Define clear structures and processes to deal with inappropriate/illegal activity whilst using digital technology [noting that these need to be cross-referenced with other school policies].
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

ROLES AND RESPONSIBILITIES

The Headmistress has a duty of care for ensuring the safety (including online safety) of members of the school community, responsibility for students is delegated to the Designated Safeguarding Lead (Director of Students) and the Director of IT for staff. The Headmistress, Designated Safeguarding Lead and Director of IT are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see below).

The managed service provider is Class Technology Solutions Ltd (CTS) responsible for ensuring that the School's technical infrastructure is secure and is not open to misuse or malicious attack; that the School meets required online safety technical requirements and that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed. Provision will be reviewed regularly by the Director of IT and the managed service Network Manager.

Teaching and support staff are responsible for ensuring that they have an up to date awareness of online safety matters and of the current School policies and practices; staff are expected to follow the School's policies on IT and Communications, Social Media and Data Protection, available in the Employment Policies Handbook.

Staff must report any suspected misuse or problem to the Director of IT and all of their digital communications with students and parents/carers and colleagues should be on a professional level.

Students are responsible for using the School's digital technology systems in accordance with the ICT Acceptable Use Policy - Students.

USE OF TECHNOLOGY – POLICY & PROCEDURE

Clear guidance on the use of technology in the classroom and beyond for all users, including staff, students and visitors that references permissions/restrictions and agreed sanctions is found in the following documents, which should be read in conjunction with this policy:

- **The ICT Acceptable Use Policy – Students**: available to students, parents/carers on the School's Extranet. A summary of this document is displayed to students at login and they must click their acceptance to continue.
- **IT and Communications Policy, Social Media Policy and Data Protection Policy:** available to staff in the Employment Policies Handbook. Staff are expected to follow these policies at all times.
- **Visitors:** are provided with and are required to digitally sign an acceptable use policy during sign in via a unique code provided at reception.

TECHNICAL PROVISION

School technical systems are managed in ways that ensure that the School meets recommended technical safety requirements and there are regular reviews and audits of the safety and security of School technical systems. Servers, wireless systems and cabling are securely located and physical access is restricted.

All users will have clearly defined access rights to School technical systems and devices. All users are provided with a username and secure password by the managed service provider, who keeps an up to date record of users and their usernames. Users are responsible for the security of their username and password. Staff are required to change their password every term.

The administrator passwords for the School's IT systems, used by the managed service provider, are available to the Director of IT and kept in a secure place.

The managed service provider ensures network health through use of Sophos anti-virus software.

The managed service provider is responsible for ensuring that software licence records are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

Internet access is filtered for all users on the School's wireless network, whether accessing this from a domain joined device or using their own device (BYOD). The managed service provider maintains Lightspeed internet filtering services on both the main and back-up internet feeds. Filtering protocols for staff, students and visitors on School and own devices are agreed between Class Technology Solutions Ltd (CTS) and the Director of IT and these are reviewed on an annual basis. Filtering is applied to ensure student safety alongside allowing the curriculum to be taught effectively and to that end different levels of filtering are applied to staff, Sixth Form students and students in the rest of the school. The managed service provider can and will run custom monitoring reports from Lightspeed in support of any Safeguarding concerns.

The School recognises that students potentially have access to 3G and 4G using their phones. Students in years 5-10 are not allowed to access their phones during the school day. Students in year 11 have access during breaktimes and in the sixth form whenever they are in the sixth form centre. Students are frequently reminded about online safety and behaviour. The behaviour policy applies to misuse of ICT in any context.

eSafe provide technical and physical monitoring for the School of all computer activity by staff and students on domain-joined devices. In the event of behaviour registering a concern eSafe has agreed protocols for communication with School staff based on the urgency and severity of the concern, which includes but is not limited to direct telephone contact with the Director of Students and the Headmistress. The Operations and Events Assistant takes on this role for external lets and is consequently DSL trained.

PROFESSIONAL DEVELOPMENT

All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and supporting policies and procedures. Online safety refresher training is delivered annually.

It is expected that some staff will identify e-safety as a training need within their professional review process and this is met through the use of accredited external provision, such as the NSPCC Online Safety Training course.

Online Safety in the Curriculum

Online safety should be present as appropriate across of the curriculum. Staff reinforce online safety messages through their teaching and in pastoral contact, to promote responsible and resilient use of digital technologies by students and ensure they are well-placed to protect themselves.

A planned online safety curriculum is provided as part of the Computer Science, Personal Development and General Studies schemes of work. This is reviewed annually by the Director of Students, Director of IT, Head of Computer Science, Head of Junior Department, Co-Ordinator of General Studies and Head of PD. Online safety messages are reinforced as part of the planned programme of assemblies and pastoral activities. Students are taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information. They are also taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. See Appendix 2.

REPORTING MECHANISMS

Discovery of unsuitable use or materials, where no illegality is identified or suspected should be reported to the Director of Staff / senior pastoral team who will work with the Director of IT and managed service provider and to investigate, decide on a course of action and recommend/apply sanctions where necessary. In the event of the incident relating to a member of staff this may be referred to the Headmistress and HR Adviser.

Where illegal materials or activities are found or suspected this should be reported to the Director of Students, if relating to students or Safeguarding. Issues regarding staff will be reported to the Headmistress. Both will then be handled in compliance with School's Safeguarding policy and procedures. As appropriate, issues related to staff will be reported by the Headmistress to the LADO/police and subsequent steps will be determined by their response and in conjunction with the School's disciplinary policies and procedures. If the Headmistress is suspected to be the perpetrator it will be reported to the Chair of Governors who will report it to the LADO/police, as appropriate.

SUPPORT FOR PARENTS & CARERS

The School recognises that some parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The School therefore seeks to provide information and awareness to parents and carers through the pastoral page on the parents' portal and other information sent home, as appropriate. Online safety is also a key element of advice given at Welcome evenings.

DATA PROTECTION

The School is fully committed to compliance with the requirements of the Data Protection Act 2018 ("the Act"), which came into force on the 23rd May 2018. The school will therefore follow procedures that aim to ensure that all employees who have access to any personal data held by or on behalf of the school, are fully aware of and abide by their duties and responsibilities under the Act.

Staff are expected to follow the School's policies on IT and Communications, Social Media and Data Protection, available in the Employment Policies Handbook.

Governor scrutiny

The Chair of Risk and Compliance scrutinises this policy to ensure that it has the relevant content. The DSL meets with this Governor at least once a term to update her on any issues. This Governor carries out regular checks of staff to ensure practice is followed. There are termly updates to all Governors from the DSL.

Covid 19. During periods of lockdown parents were responsible for the security and filtering via their own internet provider. The school reviewed the AUP to ensure that it was fit for purpose and gave advice to all teaching staff about safeguarding and online lessons.

Policy reviewer:	**Director of Students in consultation with Director of IT**
Policy last reviewed:	**Lent 2021**
Next review due:	**Lent 2022**
Audience:	**Staff/Parents**

APPENDIX 1

ICT Acceptable Use Policy – Students

Aims and Scope

- that students will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

I understand that should the School allow me to use my own digital technology in the school day/on school premises/on a school trip or visit that I will be governed by the same rules as were I to be using school ICT systems.

I understand that this Acceptable Use Policy is an extension to the school rules and forms a contract between the student and the School endorsed by their parents.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications and that files may be deleted if they pose a threat to the system or misuse is identified.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it. I will not leave my computer logged on.
- I will be aware the potential dangers of corresponding with unknown people by email or through Internet sites.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I am aware that, for my own safety, I should not arrange to meet people off-line that I have only communicated with on-line. If I decide to, I know I should do so in a public place and take an adult with me.
- I will immediately report to a responsible adult any unpleasant or inappropriate material or anything that makes me feel uncomfortable when I see it on-line.
- I will immediately report to an adult if I feel bullied or abused online or if I receive any offensive or inappropriate images, including nude or nearly nude selfies (sexting). I will not tolerate offensive behaviour from my peers and will always report it.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) make large downloads or uploads, or stream audio or video that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, social media or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

- I will use printers responsibly for my work and avoid the waste of unnecessary or irrelevant printing.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. I will recognise that what I might consider 'banter' others might find offensive or abusive.
- I will not send or take part in the preparation of text, graphics, audio or video material which is offensive, abusive, obscene or defamatory or which may be unlawful (e.g. sexting).
- I will not take or distribute still or moving images of anyone without their permission. I will not take or distribute still or moving images of the School without permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will treat computers and peripherals responsibly and immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet, I recognise that:

- I am responsible for my good behaviour.
- I understand the risks and will not try to upload, download, access or transmit any materials which are illegal or inappropriate or may cause harm or distress to myself or others.

This includes but is not limited to:

- pornographic material (that is, writing, pictures, films and video clips of a sexually explicit nature), including nude or nearly nude selfies (sexting)
- offensive, obscene, or criminal material or material which is liable to cause embarrassment to the School;
- a false and defamatory statement about any person or organisation;
- material which is discriminatory, extremist, offensive, derogatory or may cause embarrassment to others;
- confidential information about staff, students or parents (which I do not have authority to access);
- any other statement which is likely to create any legal liability (whether criminal or civil, and whether for me or the School);
- material in breach of copyright.

Nor will I try to use any programmes or software that might allow me to bypass filtering / security systems in place to prevent access to such materials.

- Access to the Internet is provided for me to conduct academic research and to communicate/collaborate with other members of the school community, using the school's mail service.
- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate. I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me and/or to put across biased or extreme views.
- At school, teachers will guide me towards appropriate materials. Outside school, families bear responsibility for such guidance as they must also exercise with information sources such as television, telephones, films, radio and other potentially offensive media.
- All internet access is subject to filtering and content control, to minimize access to inappropriate material. All internet access in school is logged, monitored and traceable.

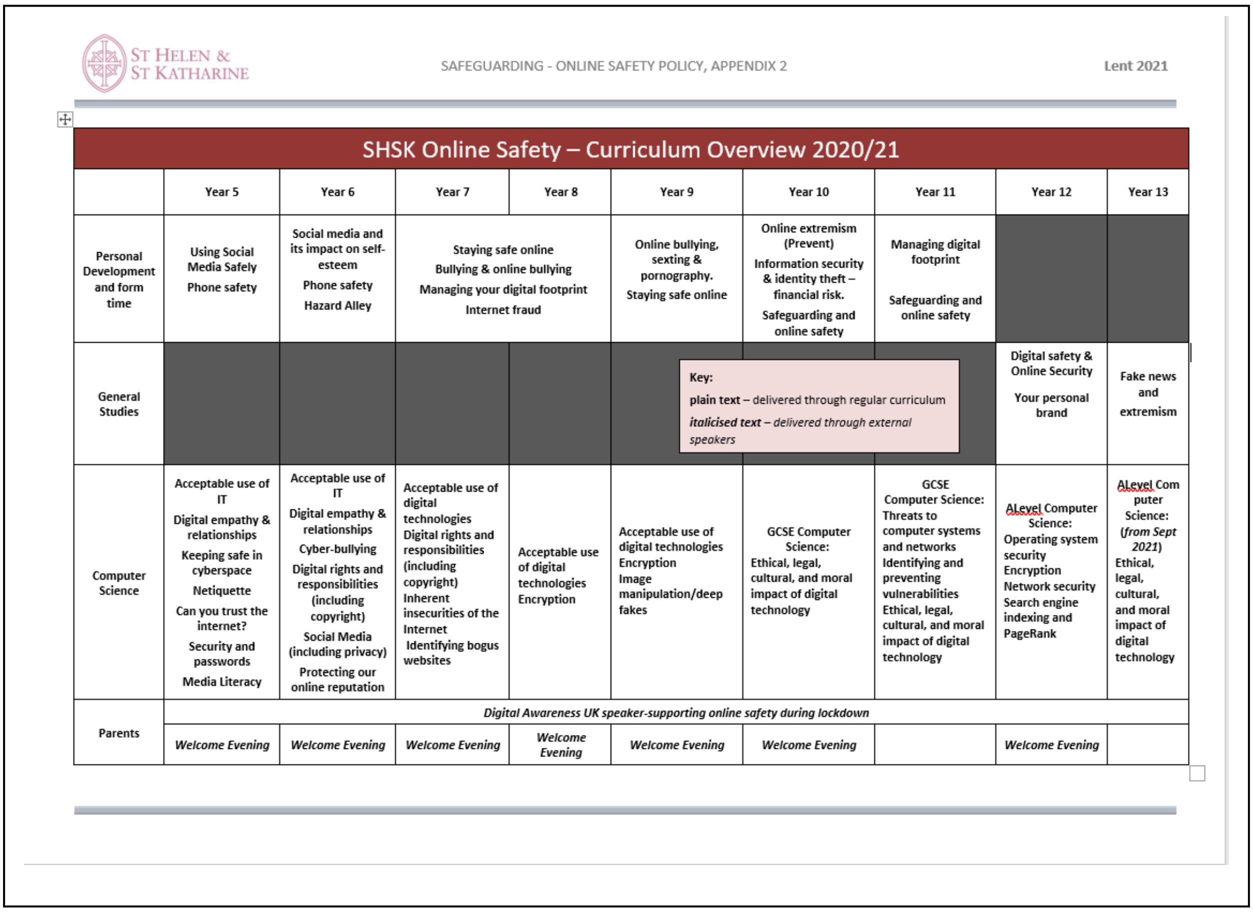
I understand that I am responsible for my actions, both in and out of school:

- I understand that the School also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would include cyber-bullying, use personal information, or transmission of offensive or extremist material, including nude/nearly nude selfies (sexting)). I understand that the School will never tolerate abusive behaviour by one student towards another.

- I will ensure that if I am joining lessons or other events remotely I will adhere to the expected standards of dress, ensure I am working in an appropriate environment, and behave courteously towards my peers and teachers in line with the School's policy and expectations of my behaviour.
-
- I understand that I must not record film or take photos during lessons, or around school (even if this is just of myself) unless given express permission to do so by a member of staff. I must not post images or videos online that have been filmed within school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, and referral to my Head of Section; Director of Students or the Headmistress.

Policy last reviewed: Lent 2021
Next review due: Lent 2022
Person responsible for review: Director of IT



ST HELEN & ST KATHARINE

SAFEGUARDING - ONLINE SAFETY POLICY, APPENDIX 2

Lent 2021

SHSK Online Safety – Curriculum Overview 2020/21

	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Year 11	Year 12	Year 13
Personal Development and form time	Using Social Media Safely Phone safety	Social media and its impact on self-esteem Phone safety Hazard Alley	Staying safe online Bullying & online bullying Managing your digital footprint Internet fraud		Online bullying, sexting & pornography. Staying safe online	Online extremism (Prevent) Information security & identity theft – financial risk. Safeguarding and online safety	Managing digital footprint Safeguarding and online safety		
General Studies								Digital safety & Online Security Your personal brand	Fake news and extremism
Computer Science	Acceptable use of IT Digital empathy & relationships Keeping safe in cyberspace Netiquette Can you trust the internet? Security and passwords Media Literacy	Acceptable use of IT Digital empathy & relationships Cyber-bullying Digital rights and responsibilities (including copyright) Social Media (including privacy) Protecting our online reputation	Acceptable use of digital technologies Digital rights and responsibilities (including copyright) Inherent insecurities of the Internet Identifying bogus websites	Acceptable use of digital technologies Encryption	Acceptable use of digital technologies Encryption Image manipulation/deep fakes	GCSE Computer Science: Ethical, legal, cultural, and moral impact of digital technology	GCSE Computer Science: Threats to computer systems and networks Identifying and preventing vulnerabilities Ethical, legal, cultural, and moral impact of digital technology	ALevel Computer Science: Operating system security Encryption Network security Search engine indexing and PageRank	ALevel Computer Science: (*from Sept 2021*) Ethical, legal, cultural, and moral impact of digital technology
Parents	*Digital Awareness UK speaker-supporting online safety during lockdown*								
	Welcome Evening	*Welcome Evening*	*Welcome Evening*	*Welcome Evening*	*Welcome Evening*	*Welcome Evening*		*Welcome Evening*	

Key:

plain text – delivered through regular curriculum

italicised text – *delivered through external speakers*