ST HELEN & ST KATHARINE

LENT 2023

1. SAFEGUARDING - ONLINE SAFETY POLICY

If you are worried about a child:

1. If it is an emergency phone 999
2. Inform the DSL Liz Bedford ebedford@shsk.org.uk / 07885458174 or any one of the DDSLs Heather Darcy, Helen Nash, Kay Taylor, Lucy Lindsay and Rachel Green (contact details in table below)
3. Alternatively, if you have significant concerns you can contact the MASH directly 0345 050 7666

If you have concerns about an adult's behaviour in or linked to school:

1. Inform the Head Rebecca Dougall head@shsk.org.uk / 01235 546502
2. Or if your concerns are about the Head, the Chair of Governors Kevan Leggett kleggett@shsk.org.uk
3. Alternatively, you can contact the LADO (see below)

Key contact details for safeguarding in the local area

Local Authority Designated Officer	Jo Lloyd TEL: 01865 810603 EMAIL: lado.safeguardingchildren@oxfordshire.gov.uk
Locality and Community Support Service (South)	TEL: 0345 2412608 EMAIL: LCSS.South@oxfordshire.go.uk
Multi-Agency Safeguarding Hub – Oxfordshire	TEL: 0345 050 7666 / 0333 014 3325 OUT OF HOURS: 0800 833408
Multi-Agency Safeguarding Hub - Berkshire	TEL: 01635 503090 EMERGENCY OUT OF HOURS: 01344786543
NSPCC Whistleblowing Advice Line	ADDRESS: Weston House 42 Curtain Road London EC2A 3NH

	TEL: 0800 028 0285 EMAIL: help@nspcc.org.uk
NSPCC Report Abuse in Education Advice Line	TEL: 0800 136 663 EMAIL: help@nspcc.org.uk

Key External Contact Details

Disclosure and Barring Service	ADDRESS: DBS customer services PO Box 3961 Royal Wootton Bassett SN4 4HF TEL: 03000 200 190 EMAIL: customerservices@dbs.gov.uk
Teaching Regulation Agency	ADDRESS: Teacher Misconduct Ground Floor South Cheylesmore House 5 Quinton Road Coventry CV1 2WT TEL: 0207 593 5393 EMAIL: misconduct.teacher@education.gov.uk
OFSTED Safeguarding Children	TEL: 0300 123 4666 (Monday to Friday from 8am to 5pm) EMAIL: CIE@ofsted.gov.uk
Independent Schools Inspectorate	TEL: 0207 6000100 EMAIL: concerns@isi.net

Key School Contact Details

Governors	**Chair of Governors** Kevan Leggett EMAIL: kleggett@shsk.org.uk **Nominated Safeguarding Governor**

	Jacqualyn Pain EMAIL: j9pain@shsk.org.uk
Designated Safeguarding Lead ("DSL") {and Deputy Designated Safeguarding Lead ("DDSL")}	**Main DSL for the School** Liz Bedford TEL: 07885 458174 EMAIL: ebedford@shsk.org.uk **Deputy DSLs** Lucy Lindsay (Junior) EMAIL: llindsay@shsk.org.uk Rachel Green (Junior) TEL: 07921 479724 EMAIL: rgreen@shsk.org.uk Kay Taylor (Lower) TEL: 07955 081647 EMAIL: ktaylor@shsk.org.uk Helen Nash (Middle) Tel: 07955 081646 EMAIL: hnash@shsk.org.uk
Designated Teacher for Looked After Children	Liz Bedford TEL: 07885 458174 EMAIL: ebedford@shsk.org.uk
Head	Rebecca Dougall TEL: 01235 546502 EMAIL: head@shsk.org.uk

SCOPE AND ASSOCIATED POLICIES

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, Relationships and Sex Education, Health and Safety, Pastoral Care, Behaviour, Work Experience, Staff Code of Conduct.

In writing the Safeguarding policies we have referred to: Keeping Children Safe in Education (September 2022) (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

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

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.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate or harmful content, for example pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users; for example; child to child 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; for example, 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.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Summary of actions

Element	Key actions
content	Filtering-Smoothwall Staff and Student AUP[1]
contact	Smoothwall, Personal Development(PD) and General Studies(GS) lessons, Computing curriculum
conduct	Smoothwall, PD and GS, AUP
commerce	Smoothwall, teacher and student education in online safety, Computing curriculum

Please see Appendix 2 for further detail on lesson content

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 Deputy Head for Staff. The Headmistress, Designated Safeguarding Lead and Deputy Head 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 IT 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 Finance and Operations 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.

All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography.

Staff must report any suspected misuse or problem to the Deputy Head and all 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:

[1] AUP Acceptable Use 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 at least once a year. Passwords for staff must be at least 15 characters in order to make them more secure.

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

The managed service provider ensures network security 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 network, whether accessing this from a domain joined device or using their own device (BYOD). The managed service provider maintains Smoothwall Filter -internet filtering service 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), the Deputy Head and the Director of Students. 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 also administers the Smoothwall Monitoring system on all network-joined devices. Any reports of concerns about students are reported to the Director of Students and concerns about staff to the Headmistress through the Smoothwall Monitor notification service. Smoothwall 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 Deputy Director of Operations takes on this role for external lets and is consequently DSL trained.

The school recognises that students potentially have access to 3G, 4G and 5G using their phones. Students in years 5-10 hand in their phones for the duration of the school day. Students in year 11 may only access their phones with the permission of a teacher. The sixth form can use them whenever they are in the sixth form centre or in lessons, with the agreement of a teacher. Students are frequently reminded about online safety and behaviour as accessing 3G, 4G and 5G will give them unfiltered access to the internet. The behaviour policy applies to misuse of digital technology in any context.

Smoothwall 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 Smoothwall 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 Deputy Director of Operations 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 at least annually through staff meetings, safeguarding updates, speakers and webinars as appropriate.

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 and webinars.

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 Computing, Personal Development and General Studies schemes of work. This is reviewed annually by the Director of Students, Deputy Head, Head of Computing, 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
Students who have breached the acceptable use policy (where no illegality is identified or suspected) should be reported to the Director of Students who will work with the Deputy Head and managed service provider to investigate, decide on a course of action and recommend/apply sanctions where necessary. It may also be appropriate to consider reporting the issue as a safeguarding matter. In the event of the incident relating to a member of staff this will be referred to the Headmistress and HR Manager. This may be recorded as a 'low level concern' (See Child Protection Policy) or subject to disciplinary action.

Where illegal materials or activities by students are found or suspected this should be reported to the Director of Students. The Director of Students will then inform the Headmistress and other agencies, for example the police or children's services, as appropriate. (See Child Protection policy)

Issues regarding staff will be reported to the Headmistress. These will be handled in compliance with School's Child Protection 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.

GDPR

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 of May 2018 and the UK General Data Protection Regulation (GDPR). 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. (See Data Protection Policy).

Staff are expected to follow the school's policies on IT and Communications, social media and Data Protection, available in the Employment Policies Handbook.

DPA and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare. If in any doubt about sharing information, staff should speak to the Director of Students (DSL) or a Head of Section (DDSL). Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare of children.

GOVERNOR SCRUTINY

The Chair of Governance scrutinises this policy to ensure that it has the relevant content. The DSL meets with this Governor at least once a term to update them 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.

Policy reviewer:	**Director of Students in consultation with Deputy Head**
Policy last reviewed:	**Lent 2023**
Next review due:	**Lent 2024**
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 of 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 online (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 semi-nude pictures (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) to 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 (including misogynistic), 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.
- I will not use any 3rd party software like Virtual Private Networks (VPNs) or any other anonymous browser enabling software to deliberately bypass the school's filtering/security systems thus accessing inappropriate material/websites.

- 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 images (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 2023
Next review due: Lent 2024
Person responsible for review: Deputy Head

APPENDIX 2

SHSK Online Safety – Curriculum Overview 2022/23									
	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Year 11	L6	U6
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 Online Piracy Internet fraud and data protection		Online Stress and Fear of Missing Out, sexting & Staying safe online	Information security & identity theft. Online Blackmailing awareness– Safeguarding and online safety and pornography	Managing digital footprint Safeguarding and online safety	Digital safety & Online Security Safeguarding and online safety Professional Identity	Information security & identity theft – financial risk.
Computer Science	Acceptable use of IT Joining in with online communities Sharing information online Fake profiles and fake news Sensible searching Passwords & app security Copying content	Acceptable use of IT Online communication Positive use of social media Dealing with online issues Screen Time Digital footprint & online reputation Check your facts Permissions & privacy settings Copyright & acknowledging sources	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 Untrustworthy websites/cybersquatting/typosquatting	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	A Level Computer Science Operating system security Encryption Network security Search engine indexing and PageRank	A Level Computer Science: Network security Ethical, legal, cultural, and moral impact of digital technology
Parents	*Regular updates and online safety tips through the weekly mailing including highlighting the Teen tips well-being hub webinars*								
	Welcome Evening	*Welcome Evening*	*Welcome Evening*	*Welcome Evening*	*Welcome Evening*	*Welcome Evening*		*Welcome Evening*	