Online Safety Policy

St Laurence School Academy Trust

Date of last review:	March 2023 Approved C&E	**Review period:**	1 year
Date of next review:	March 2024	**Owner:**	Assistant Headteacher

Introduction

St Laurence School is committed to the safeguarding of all in its community, in line with our mission statement that 'People are our Treasure'.

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2022, and its advice for schools on:

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

Aims

St Laurence School aims to:

- have robust processes in place to ensure the online safety of students, staff, volunteers and governors;
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology*;
- establish clear procedures to identify, intervene and escalate an incident, where appropriate.

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

- **Content** – being exposed to all forms of online sexual abuse, illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalization and extremism,
- **Contact** – being subjected to harmful online interaction or sexual abuse 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 (cyberflashing) and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

* For the purposes of this policy, Smart Technology refers to all devices controlled via a remote and connected via the internet or Bluetooth.

Roles and Responsibilities

The Governors

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Community and Ethos Committee (C&E) will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs via MyConcern as provided by the Designated Safeguarding Lead (DSL).

All governors will:

- ensure that they have read and understand this policy;
- agree and adhere to the terms on acceptable use of the school's ICT systems and the internet;

- ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead and Deputy Designated Safeguarding Lead for online safety

Details of the school's DSL and DDSL for Online Safety are set out in the child protection and safeguarding policy as well as relevant job descriptions.

The DDSL For Online Safety 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 and Keeping Children Safe in Education 2022
- For monitoring email alerts from Smoothwall filtering system and recording concerns on MyConcern to be dealt with appropriately in line with this policy
- Ensuring that any online safety incidents are logged on MyConcern 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
- Adding regular updates for parents/carers to the bulletin on online safety
- 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

The ICT Manager

The ICT Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading and/or running of potentially dangerous files.
- Ensuring the school is protected from external threats via the firewall.
- Ensuring that the school's ICT systems are secure and protected against viruses, malware, email phishing and that such safety mechanisms are updated regularly.
- Regularly conducting security checks and monitoring the school's ICT systems, organising an annual full security audit by an external IT company.

- Ensuring that any online safety incidents are reported to the DDSL for Online Safety.
- Ensuring that any incidents of cyber-bullying are reported to the DDSL for Online Safety.
- Ensuring that any incidents where network accounts or IT security has been compromised are reported to the Director of Finance and Operations for appropriate action.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that students follow the school's terms on acceptable use
- Working with the DSL/DDSL to ensure that any online safety incidents are logged on MyConcern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

Parents

Parents are expected to:

- notify a member of staff or the Headteacher of any concerns or queries regarding this policy;
- to engage with their child about their online behaviour;
- ensure their child has read, understood and agreed to the terms of the school's Social Media Policy and Acceptable Use of the school's ICT systems and internet.

Parents can seek further guidance on keeping children safe online on the school website in the Online Safety section and via the parent/carer bulletin.

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating students about online safety

Students will be taught about online safety as part of the PSHE and Computing curriculum including knowledge of/about:

- their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online;
- online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online;
- not to provide material to others that they would not want shared further and not to share personal material which is sent to them;
- what to do and where to get support to report material or manage issues online;
- the impact of viewing harmful content;

- that specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners;
- sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including custodial sentences;
- how information and data is generated, collected, shared and used online;
- how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours;
- how people can actively communicate and recognize consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online);

The safe use of social media and the internet will also be covered during tutorial and in other subjects where appropriate.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

Educating parents about online safety

The school will raise parents' awareness of internet safety in briefings, letters, the parent/carer bulletin and in information via our website. Parents also have been invited to have an account on National Online Safety, to which we subscribe.

This policy will be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DDSL for Online Safety.

Concerns or queries about this policy can be raised with the Headteacher.

Some parents allow their child to use personal data. The school accepts no responsibility for unfiltered access if a student chooses to use personal mobile data on the school site, outside of the school WiFi protection, to access content.

Cyber-bullying

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others.

Students are encouraged to report any incidents of cyber-bullying to their tutor, head of House or via the school email stopbullying@st-laurence.com

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their tutor groups and within PSHE and Computing curriculum time.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of the annual safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.

The DSL/DDSL for Online Safety will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, the staff member must liaise with the DSL/DDSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to adhere to the school's Acceptable User Policy. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above, this includes students' use of the WiFi on their mobile devices.

More information is set out in the acceptable use agreements.

Students and staff using mobile devices in school

See separate Mobile Device policy

Staff using work devices/accessing the school systems remotely

All staff members will take appropriate steps to ensure their devices/remote access desktops 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 – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

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 the ICT manager.

How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in related policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct and disciplinary policy procedure. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

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 through the staff bulletin.

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:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - 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 students can recognize dangers and risks in online activity and can weigh the risks up
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSL for Online Safety 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.

Monitoring arrangements

Smoothwall Filtering and Monitoring is used as a tool to monitor inappropriate or illegal use of the school internet (including WiFi). Email alerts are sent to the DDSL for Online Safety.

MyConcern is used to log behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the DDSL for Online Safety. At every review, the policy will be shared with the governing board (C&E Committee). The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet Acceptable Use Policy
- Mobile Device Policy
- Social Media Policy

Appendix A – Definitions

Radicalisation and extremism
Radicalization is the process through which a person comes to support or be involved in extremist ideologies. Extremism is vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs.

Cyber-bullying
Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Smart technology
The word "SMART" refers to "self-monitoring, analysis, and reporting technology". It is a technology that uses artificial intelligence, machine learning, and big data analysis.
For the purposes of this policy, Smart Technology refers to all devices controlled via a remote and connected via the internet or Bluetooth.

Fake news
False stories that appear to be news, spread on the internet or using other media, usually created to influence political views or as a joke.

Pfishing
The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Malware
Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.

CEOP
Child Exploitation and Online Protection Centre
CEOP is a law enforcement agency who is engaged in keeping children and young people safe from sexual abuse and grooming online.

Cyberflashing
A crime which involves sending obscene pictures to strangers online.

Online Sexual Abuse
Any type of sexual abuse that happens over the internet or on a mobile device.

Appendix B – Guidance and Support

At St Laurence School, we have subscribed to a new online resource for the whole community. **'National Online Safety'** is a comprehensive online safety programme with resources on:

- setting up parental controls for all models of phone and other devices;
- online safety guides to all social media platforms;
- online gaming;
- how to report a problem.

In order to create a personal account, please use this link:

https://nationalonlinesafety.com/enrol/st-laurence-school

You can find out more about how children use social media, the apps they use, the risks they face, how to use privacy settings, and advice and tips about how to talk to your children at:

• www.childnet.com/sns

• www.internetmatters.org

• www.nspcc.org.uk/onlinesafety

• www.parentzone.org.uk

• www.thinkyouknow.co.uk/parents

• www.askaboutgames.com

To make a report

If you are concerned about online grooming or sexual behaviour online?
Contact CEOP:
www.ceop.police.uk

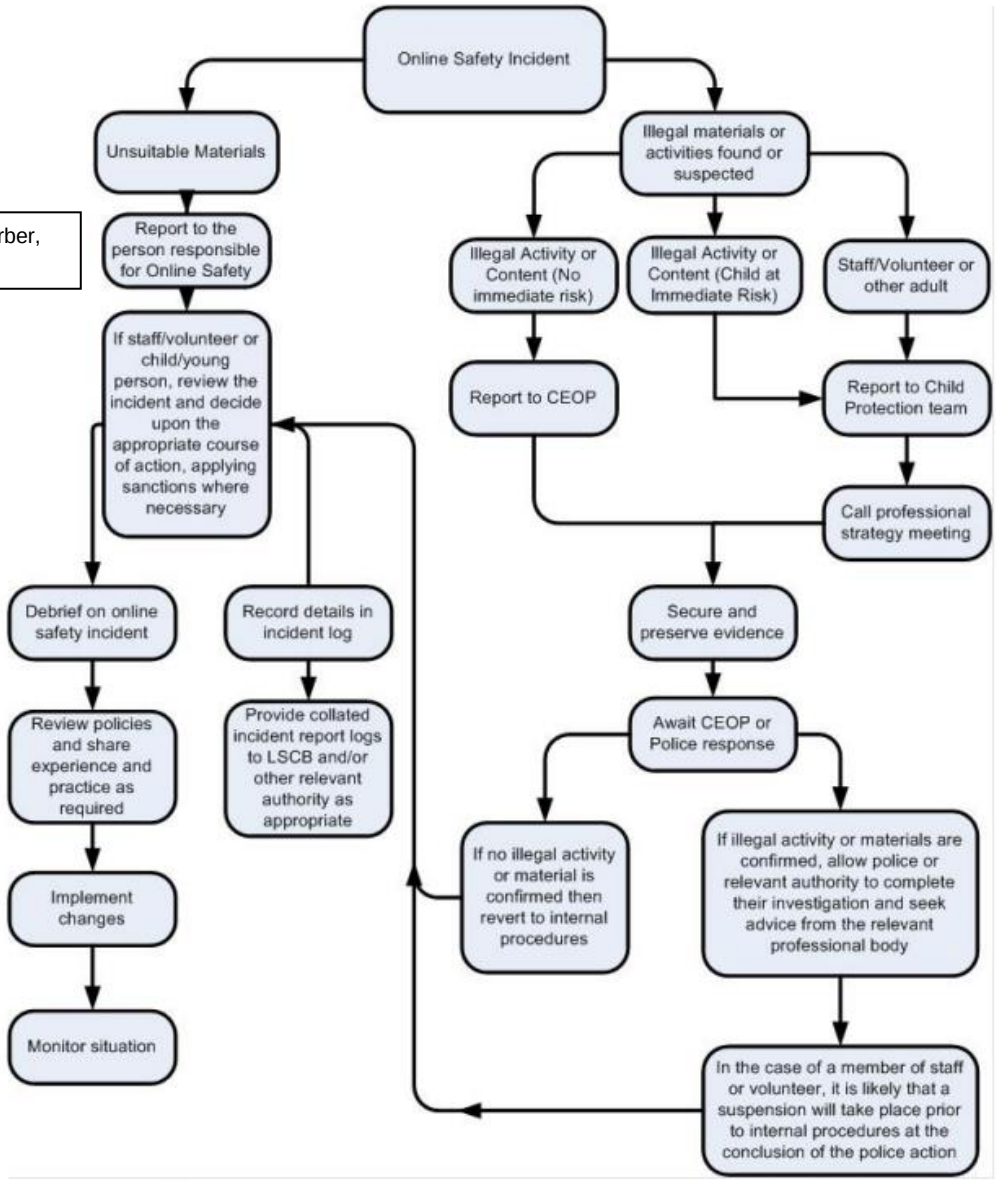
If you stumble across criminal sexual or obscene content on the internet you should report it to the Internet Watch Foundation:
www.iwf.org.uk

Social Media Age Restrictions

13 – Twitter, Facebook, Instagram, Pinterest, google+, Tumblr, reddit, Snapchat, Secret
14 – Linkedin
16 – Whatsapp
17 – Vine, Tinder
18 – Path
18 (13 with parental permission) – YouTube, Keek, Foursquare, WeChat, Kik, Flickr

Appendix C – Online Safety incident Flow chart

Laura Barber, DDSL



Key:
CEOP Child Exploitation and Online Protection.
LSCB Local Safeguarding Children Board.

Appendix D – Annex D from Keeping Children Safe in Education 2022 – Online Safety

Information and support

There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Advice for governing bodies/proprietors and senior leaders

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalization
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalization - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on, and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring
- Department for Digital, Culture, Media & Sport (DCMS) Online safety guidance if you own or manage an online platform provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.
    - Department for Digital, Culture, Media & Sport (DCMS) A business guide for protecting children on your online platform provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- National cyber security centre guidance on how to set up and use video conferencing
- UK Safer Internet Centre guidance on safe remote learning

Support for children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Parental support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalization.
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online.
- Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and

carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online.
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games.
- Parentzone provides help for parents and carers on how to keep their children safe online.
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations.
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online.