



## **Local Arrangements for Online Safety at St Stephens**

### **CofE First School**

(to be read in conjunction with CRST Online Safety Policy)

OUR VISION:

WE ARE COMMITTED TO THE CHRISTIAN ETHOS - EVERY CHILD IS SPECIAL IN THE EYES OF GOD AND WE TEACH THAT ALL PEOPLE SHOULD LOVE, CARE FOR AND RESPECT ONE ANOTHER AND OUR PLANET.

*It is our ambition that all our pupils use our 6 Christian values **Love, Compassion, Forgiveness, Integrity, Community** and **Respect** to achieve our vision and mission.*

**'A New Commandment I give you, 'Love one another as I have loved you.' John 13:34**

It is from this Commandment and the teachings of Jesus that we teach our children the six Christian values.

<b>Recommended by:</b>	Principal
<b>Recommendation Date:</b>	21 <sup>st</sup> September 2025
<b>Ratified by:</b>	<b>LAGB</b>
<b>Signed:</b>	
<b>Position on the Board:</b>	Chair of LAGB
<b>Ratification Date</b>	21 <sup>st</sup> September 2025
<b>Next Review:</b>	September 2026
<b>Policy Tier</b>	School

## **Rationale**

**The purpose of this document is to support the Central Region Schools Trust online safety policy. It will aim to:**

- set out the key principles expected of all members of our school community with respect to the use of computing and ICT-based technologies;
- safeguard and protect our children and staff;
- assist our school staff when working with children, to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice;
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use;
- have clear structures to deal with online abuse such as cyber-bullying which are cross referenced with other school policies;
- ensure that all members of our school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken;
- minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

**The main areas of risk for our school community can be summarised as follows:**

### **Content**

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

### **Contact**

- Grooming
- Cyber-bullying in all forms
- Identity theft and sharing passwords

### **Conduct**

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (Internet or gaming)
- Child on child abuse including nude image sharing (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (care or consideration for intellectual property and ownership - such as music and film)

### **Commerce**

- Gambling, including practice of 'loot boxes' in online gaming

- Adverts, particularly inappropriate advertising
- Phishing scams

## **Education and curriculum**

### **School online safety curriculum**

This school has a clear, progressive online safety education programme as part of the computing curriculum and also the PSHE curriculum. It is based on the project Evolve curriculum, devised and designed by the UK Council for Internet Safety and the SWGfL. This covers a range of skills and behaviours appropriate to their age and through this aims to:

- plan careful Internet use to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- teach pupils about their responsibilities through an end-user acceptable use agreement (AUA) which every pupil will be reminded of at the beginning of each lesson technology is used.
- ensure staff model safe and responsible behaviour in their own use of technology during lessons;
- ensure that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- ensure that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include risks in pop-ups; buying on-line; on-line gaming / gambling.

### **Staff and governor training**

St Stephens CE First School:

- Ensures staff and governors know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Provides all teaching staff with secure cloud storage (one drive) and an encrypted USB stick to ensure data is secure.
- Makes regular training available to staff and governors on online safety issues and the school's online safety education program, including information and training on the monitoring and filtering in place on the school system;
- Provides all new staff (including those on university/college placement and work experience) with information and guidance on the E safety policy and the school's acceptable use agreement (AUA).

### **Parent awareness and training**

St Stephens CE First School

- provides a programme of advice, guidance and training for parents, including:
- information leaflets, in-school newsletters, information and advice on the school web site;
- suggestions for safe Internet use at home;
- provision of information about national support sites for parents.

## **Expected conduct and incident management**

### **Expected conduct :**

At St Stephens CE First School, all users:

- Are responsible for using the school systems in accordance with the relevant school policies;

- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences;
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school;
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking and/or use of images and on cyber-bullying.

Staff are responsible for reading both the school's Trust Online Safety Policy, the local arrangements for online safety document, and using the school computing systems accordingly, including the use of mobile phones, and hand held devices.

Pupils should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/carers should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

### **Incident management**

In this school and in line with the Central Region Schools Trust Online Safety Policy:

- there is strict monitoring (through the use of our online monitoring software 'SENSO') application of the online safety policy and a differentiated and appropriate range of sanctions, (though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions)
- the network is filtered (through the use of 'netsweeper'). All users are assigned to one of 3 groups, pupil, adult or staff. Each group has appropriate filters in place. Requests to 'unblock' websites should be made thorough the DSL or the Safeguarding lead, who will check the website is appropriate and then send a request to the IT team.
- sanctions and flow chart of actions to be followed in appendix c taken from SWGfL
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (e.g. the Local Authority, other schools and where appropriate, the police)
- monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school. The records are reviewed/audited and reported to the school's senior leaders and governors
- parents/carers are informed of online safety incidents involving pupils for whom they are responsible. Where possible, this would happen on the day of the incident as it is a crucial part of our safeguarding process.
- Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

## **Password policy**

- At St Stephens CE First School, we make it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- All pupils have their own unique username and passwords.

## **Social networking**

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to the school community
- Personal opinions should not be attributed to the school or Local Authority
- They ensure their use of social networking sites is respectable and appropriate at all times
- Personal profiles do not identify their place of work
- They do not use a work email to sign up to non-work related web-accounts
- They do not have contact with students using social media
- They do not add pupils as friends or respond to friend requests from pupils
- Secure and suitable strength passwords are used
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

## **Equipment and Digital Content**

### **Personal mobile phones and mobile devices**

- Mobile phones brought into school are entirely at the staff member, pupils', parents' or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Pupil mobile phones are not allowed in school. If they are brought into school they should be safely secured, and a parent should be informed of school policy at the end of the day. All staff and visitors are requested to keep their phones in secure spaces (cupboards, offices, bags) and use them only during break times in staff work rooms and outside of the school premises.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

### **Staff use of devices**

- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional or personal capacity.
- Staff will use a school phone where contact with pupils, parents or carers is required.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken. Staff members may be required to use a mobile phone for school duties, for instance in case of emergency during off-site activities.

### **Digital images and video**

#### **In this school:**

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

### **Cyber Security**

#### **In this school:**

- All staff use secure passwords, which are not shared with anyone as detailed above.
- All staff receive training concerning cyber threats, including what this may entail, what the dangers to them are and how they can be avoided.
- System is managed by CRST IT team, who put relevant cyber security systems and programs in place.

These Local Arrangements will be reviewed in a timely manner in accordance with the Central Region Schools Trust Online Safety Policy.

Appendix A

Role	Key Responsibilities
Principal Sarah Callanan	<ul style="list-style-type: none"> <li>• To take overall responsibility for online safety provision.</li> <li>• To take overall responsibility for data and data security.</li> <li>• To ensure the school uses an approved, filtered Internet service, which complies with current statutory requirements.</li> <li>• To be responsible for ensuring that all teaching and non-teaching staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant.</li> <li>• To be aware of procedures to be followed in the event of a serious online safety incident.</li> <li>• To receive regular monitoring reports from the online safety lead.</li> <li>• To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures.</li> </ul>
Online safety lead Computing Lead Lauren Cullen	<ul style="list-style-type: none"> <li>• To take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.</li> <li>• To promote an awareness and commitment to online safeguarding throughout the school community.</li> <li>• To ensure that online safety education is embedded across the curriculum.</li> <li>• To liaise with Academy technical staff on the latest developments.</li> <li>• To communicate regularly with SLT and the designated online safety governor / governing body committee to discuss current issues, review incident logs and filtering.</li> <li>• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident.</li> <li>• To audit online safety at least annually (using 360 safe or similar).</li> <li>• To ensure that E Safety is continually monitored via SENSO.</li> <li>• To facilitate training and advice for all staff.</li> <li>• To liaise with the local authority (LA) and other relevant agencies.</li> <li>• To be regularly updated regarding online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:               <ul style="list-style-type: none"> <li>□ sharing of personal data.</li> <li>□ access to illegal / inappropriate materials.</li> <li>□ inappropriate on-line contact with adults / strangers.</li> <li>□ potential or actual incidents of grooming.</li> <li>□ cyber-bullying and use of social media.</li> </ul> </li> <li>• To oversee the delivery of the online safety element of the computing curriculum.</li> <li>• To liaise with the PSHE lead on a regular basis</li> </ul>
Governors Online Safety Governor Paul Lawlor, Safeguarding Governor	<ul style="list-style-type: none"> <li>• To ensure that the school follows all current online safety advice to keep the children and staff safe.</li> <li>• To approve the 'Local Arrangements for Online Safety' document and review the effectiveness of this.</li> <li>• To support the school in encouraging parents and the wider community to become engaged in online safety activities.</li> </ul>

<p>Network manager / technician Daniel Carpenter</p>	<ul style="list-style-type: none"> <li>• To report any online safety related issues that arises, to the online safety lead.</li> <li>• To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed.</li> <li>• To ensure that provision exists for misuse detection and malicious attack eg keeping virus protection up to date.</li> <li>• To ensure the security of the school computer system.</li> <li>• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices.</li> <li>• To ensure the school's policy on web filtering is applied and updated on a regular basis.</li> <li>• To ensure that he/she keeps up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.</li> <li>• To ensure that the use of the network / Virtual Learning Environment / remote access / e-mail is regularly monitored in order that any misuse / attempted misuse can be reported to the online safety lead/SLT for investigation / action / sanction .</li> <li>• To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.</li> <li>• To keep up-to-date documentation of the school's e-security and technical procedures</li> </ul>
<p>Teachers</p>	<ul style="list-style-type: none"> <li>• To embed online safety issues in all aspects of the curriculum and other school activities.</li> <li>• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).</li> <li>• To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.</li> </ul>
<p>All staff</p>	<ul style="list-style-type: none"> <li>• To read, understand and help promote the Central Region Schools Trust Online Safety Policy and the Local Arrangements for Online Safety document.</li> <li>• To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.</li> <li>• To report any suspected misuse or problem to the online safety lead.</li> <li>• To maintain an awareness of current online safety issues and guidance e.g. through CPD.</li> <li>• To model safe, responsible and professional behaviours in their own use of technology.</li> <li>• To ensure that any digital communications with pupils should be on a professional level and only through school based systems (Seesaw), and never through personal mechanisms, e.g. email, text, mobile phones etc.</li> </ul>

Pupils	<ul style="list-style-type: none"> <li>• Read, understand and adhere to the pupil acceptable use policy.</li> <li>• Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.</li> <li>• Understand the importance of reporting abuse, misuse or access to inappropriate materials.</li> <li>• To know what action to take if they or someone they know feels worried or vulnerable when using online technology.</li> <li>• To know and understand school arrangements on the use of mobile phones, digital cameras and hand held devices.</li> <li>• To know and understand school arrangements on the taking / use of images and on cyber-bullying.</li> <li>• To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Local Arrangements for Online Safety document covers their actions out of school, if related to their membership of the school.</li> <li>• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home.</li> </ul>
Parents/carers	<ul style="list-style-type: none"> <li>• To support the school in promoting online safety and endorse the parents' acceptable use agreement which includes the pupils' use of the internet and the school's use of photographic and video images.</li> <li>• To read, understand and promote the school pupil acceptable use agreement with their children.</li> <li>• To access the school website / on-line student / pupil records in accordance with the relevant school acceptable use policy.</li> <li>• To consult with the school if they have any concerns about their children's use of technology.</li> </ul>
External groups	Any external individual / organisation will be made aware of the school's acceptable use agreement (AUA) prior to using any equipment or the internet within school.

**Acceptable Use Agreement (AUA)**

This is how we stay safe when we use computers and mobile devices.:

- I will take care of computers and other devices.
- I will ask for help if I am not sure what to do or if I think I have done something wrong.
- I will be responsible for my behaviour when using technology because I know that if I break the rules I might not be allowed to use a computer or other devices.
- I will freely choose from a selection of programmes and apps.
- I will ask an adult if I want to use the computer or mobile devices.
- I understand that my use of technology (especially when I use the Internet) will be supervised and monitored.
- I will keep my password safe and I will not use another persons password (even with their permission).
- I will not give out a copy of my own details (name, address etc) and I will not arrange to meet anyone that I have met online.
- An adult must check any messages I send and receive.
- I will not take or share images of anyone without their permission.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell an adult immediately.

Appendix C

Responding to incidents of misuse – flow chart (taken from SWGfL)

