Insert school Logo

Online Safety Policy

This policy has been approved and adopted by the Xavier Catholic Education Trust in Oct 2026

Committee Responsible: Risk & Audit Committee
To be reviewed in Oct 2027

N.B. This policy is a supplemental policy to the Child Protection and Safeguarding Policy. This policy is a framework and should be seen as a template for developing a policy that meets the needs and context of individual schools. Please review the template and amend with information relevant to the individual school context.

Areas for attention/amendment are highlighted in yellow.

Contents

Key Contacts 2
Mission and principles 3
Scope 4
Monitoring and Review 5
Roles and Responsibilities 5
Education and engagement with learners 11
Training and engagement with staff 13
Awareness and engagement with parents and carers 13
Reducing Online Risks 13
Safer Use of Technology 14
Managing internet access 15
Filtering and monitoring 15
Managing personal data online 17
Security and management of information systems 18
Password policy 18
Managing the safety of our website 18
Publishing images and videos online 19
Managing email 19
Management of learning platforms 20
Management of applications (apps) used to record children's progress 20
Use of Social Mediaby inserting 21
Mobile Technology: Use of Personal Devices and Mobile Phones 25
Responding to Online Safety Incidents and Concerns 29
Procedures for Responding to Specific Online Incidents or Concerns 31
Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation) 34
Indecent Images of Children 35
Cyberbullying 37
Online hate 37
Online radicalisation and extremism 37
Responding to an Online Safety Concern Flowchart 38
Useful Links 39

Key Contacts

Designated Safeguarding Lead (DSL) is:
Contact details:

Deputy DSL(s) is/are:
Contact details:

The Online Safety coordinator is
Contact details:

The IT Network Manger is:
Contact details:

The Headteacher is:
Contact details:

The Chair of Governors is:
Contact details:

The nominated child protection governor is:
Contact details:

The Xavier Catholic Education Trust Safeguarding Compliance Director is: Anne Halliday
Contact details: 07840 448692; email: a.halliday@xaviercet.org.uk

The CEO Xavier Catholic Education Trust is: James Kibble
Contact details: 07840 448692; email: j.kibble@xaviercet.org.uk

Mission and principles

Our mission is to inspire, nurture and fulfil the calling of every person we encounter and the potential of every school we serve; growing together in faith, hope and love.
Everything we do in Catholic education is to ensure that every child we teach and every person we work with has the opportunity to realise their own calling and become the best version of themselves.

Our aim is to enable potential with the highest-quality provisions, to go out into the world and make our unique contribution for the greater good of all God's people here on Earth.
This is particularly important for the children, who are at the start of their journey to fulfil their calling and only get one chance at experiencing high-quality provision in school.

Insert context for school

For example –

At Holy Family School, we encourage all our children to be active learners, to develop ideas and work to the very best of their abilities. We work with home and parish, to build and nurture their confidence, self-esteem, creativity and skills within an inclusive and caring Christian environment.

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. Holy Family Catholic Primary School endeavours to highlight the benefits and risks of using technology and provides Safeguarding and education for users to enable them to control their online experience.

This policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2026,'Working Together to Safeguard Children' 2026, 'Teaching Online Safety in Schools' 2023, 'Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges' 2026, 'Generative AI: product safety expectations' 2026 and the local Surrey Safeguarding Children Partnership Procedures.

This document should be read in conjunction with other relevant policies including, but not limited to, the Xavier Child Protection and Safeguarding policy, Behaviour policy, Relationship and Sex Education policy, Xavier IT User Requirements, Xavier Code of Conduct and Whistleblowing policy.

The purpose of *insert name of school* online safety policy is to:

- Safeguard and promote the welfare of all members of the *insert name of school* community online;
- Identify approaches to educate and raise awareness of online safety throughout our community;
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology;
- Identify clear procedures to follow when responding to online safety concerns;
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching and learning and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.

Insert name of school identifies that the breadth of issues classified within online safety are considerable but can be broadly categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,
- **Contact:** being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: 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 behavior that increases the likelihood of, or causes, harm, for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Scope

Insert name of school recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.

Insert name of school acknowledges 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 making or sharing of nudes or semi-nudes, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

Insert name of school acknowledges that the internet and associated devices, such as computers, tablets, mobile phones, games consoles and other personal electronic devices are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks.

Insert name of school will empower our learners to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.

This policy applies to all members of the insert name of school community (including staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as “staff” in this policy) as well as learners and parents/carers who have access to our digital technology, networks and systems, whether on-site or remotely.

This policy will help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform.

This policy applies to all access to the internet and use of technology, including mobile technology, or where learners, staff or other individuals have been provided with setting-issued devices for use, both on and off-site.

All members of the school community are made aware of our expectations regarding safe and appropriate behaviour online. This is clearly outlined in our Xavier IT User Requirements which all members of the school community are expected to sign up to.

Monitoring and Review

Technology and risks and harm related to it evolve and change rapidly; as such *insert name of school* will review this policy at least annually. The policy will be revised following any national or local policy updates or developments, local concerns and/or any changes to our technical infrastructure.

We will ensure there are appropriate filters and monitoring systems on school devices and school networks. The senior leader responsible for filtering and monitoring will review their effectiveness annually and evidence of the review will be retained. The Designated Safeguarding Lead and IT staff will contribute to the review.

We will evaluate online safety mechanisms to ensure that this policy is consistently applied. Any issues identified will be incorporated into our action planning.

We will ensure the leadership team, staff and volunteers receive online safety training and have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should ensure that all governors and trustees receive appropriate safeguarding and child protection (including online) training at induction.

To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.

The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the governing body.

Roles and Responsibilities

The Designated Safeguarding Lead (DSL) is recognised as holding overall lead responsibility for online safety;

Insert name of school recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The Leadership Team will:

Create a culture that incorporates online safety throughout all elements of school life.

Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.

Implement appropriate and up-to-date policies regarding online safety which address acceptable use of school devices and networks and personal device use in school, child-on-child abuse, use of social media and mobile technology.

Ensure that policies and procedures are followed by all staff.

Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to safeguarding principles.

Liaise with the DSL and online safety coordinator on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information.

Support the DSL by ensuring they have enough time and resources to carry out their responsibilities.

Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the Trust Board, DSL, governors and senior leadership team to ensure a GDPR-compliant framework for storing data, helping ensure that safeguarding is always put first and data-protection processes support careful and legal sharing of information.

Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.

Undertake an annual review of the school approach to online safety and undertake appropriate risk assessments, as required, regarding the safe use of technology on site and for remote learning which reflects the risks children face.

Audit and evaluate online safety practice to identify strengths and areas for improvement.

Ensure all staff receive online safety training at induction (which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) which is regularly updated. In addition, all staff will receive online safety updates as required to provide them with relevant skills and knowledge to safeguard children effectively.

Ensure that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant. Work together to ensure that all new and existing devices are configured and stored securely.

Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety.

Support staff to ensure that online safety is embedded within a progressive whole-setting curriculum which enables all learners to develop an appropriate understanding of online safety.

Ensure all children are supported to report concerns, including about harmful sexual behaviour, freely. Ensure that concerns are taken seriously and dealt with swiftly and appropriately, and that children are confident that this is the case. Ensure that comprehensive records of all concerns and allegations are kept.

Ensure the school website meets statutory requirements.

The Designated Safeguarding Lead (DSL) will:

Take lead responsibility for Safeguarding, including online safety.

Work alongside the Online Safety Coordinator to ensure an effective safeguarding approach. (remove if the DSL is the Online Safety Coordinator)

Work alongside IT staff and the senior leader responsible for filtering and monitoring, to ensure processes and procedures are effective and ensure learner safety while using school devices and networks. Reviews of filtering and monitoring will take place annually and a record of review will be retained. (Reword if DSL is the senior leader responsible for filtering and monitoring).

Be responsible for receiving and responding to reports of online safety incidents. Ensure referrals are made to relevant external partner agencies, as appropriate.

Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities, and that a coordinated whole-school approach is implemented.

Access regular and appropriate online safety training and support to ensure they understand the unique risks associated with online safety and be confident that they have the relevant and up-to-date knowledge required to keep learners safe online.

Receive regular updates on online safety issues and be aware of local and school trends.

Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.

Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.

Ensure the DfE guidance Keeping Children Safe in Education 2026 Part 5 is followed throughout the school and that staff maintain a zero-tolerance approach to sexual violence and sexual harassment.

Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.

Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.

Ensure that online safety is promoted to parents, carers and the wider community through a variety of channels and approaches.

Ensure all staff are aware of the procedures that need to be followed in the event of an online safety or cyberbullying concern. Maintain records of online safety concerns, as well as actions taken, as part of the setting's safeguarding recording mechanisms.

Monitor online safety incidents to identify gaps and trends and use this data to update school policies and procedures.

Report online safety concerns, as appropriate, to the Leadership team. Work with the Leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.

Meet regularly with the Senior Leadership Team and technical staff to discuss current issues, review incident logs and filtering and monitoring reports.

Meet regularly with the governor with lead responsibility for safeguarding.

The Trust Board will:

Approve this policy and review its effectiveness.

Support the school in encouraging parents and the wider community to become engaged in online safety activities.

Incorporate online safety into regular discussions of safeguarding.

Ensure a GDPR-compliant framework for storing data, helping ensure that safeguarding is always put first and data-protection processes support careful and legal sharing of information.

Ensure all governors and trustees receive appropriate safeguarding and child protection training, including online safety, at induction.

Ensure all staff receive safeguarding and child protection training, including online safety, at induction in line with advice from Surrey Safeguarding Children Partnership which is regularly updated and receive safeguarding and child protection updates (for example, via email, e-bulletins and staff meetings), as required, but at least annually.

Ensure appropriate filters and monitoring systems are in place and the filtering and monitoring provision is reviewed and recorded, at least annually.

Ensure children are taught about safeguarding, including online safety, as part of a broad and balanced curriculum. Ensure the curriculum is tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs and/or disabilities.

The Local Governing Committee will:

Ensure that they know the policy is in place and understand how the policy is managed at Trust Level.

The Local Governing Committee should take measures to ensure their school has appropriate cyber security and filtering and monitoring systems in place. Governors will ensure checks of these systems are undertaken annually.

Staff will:

Understand that online safety is a core part of safeguarding; as such it is part of everyone's responsibility.

Know who the Designated Safeguarding Lead and Online Safety coordinator are. (Remove if DSL is Online Safety Co-ordinator)

Contribute to the development of our Online Safety policies.

Read and adhere to our Online Safety policy and Xavier IT User Requirements in conjunction with the school's Child Protection and Safeguarding policy.

Sign the Xavier IT User Requirements.

Take responsibility for the security of IT systems and the electronic data they use or have access to.

Model good practice when using technology with learners.

Maintain a professional level of conduct in their personal use of technology, both on and off site.

Embed online safety education in curriculum delivery wherever possible.

Have an awareness of a range of online safety issues and how they may be experienced by the learners in their care.

Identify online safety concerns and take appropriate action by following the school safeguarding policies and procedures. Record online safety incidents in the same way as any safeguarding incident.

Know when and how to escalate online safety issues, including reporting to the DSL and signposting learners and parents/carers to appropriate support, internally and externally.

When overseeing the use of technology in school or setting as homework tasks, remind about safe use, monitor what children are doing and consider potential dangers and the age-appropriateness of websites.

Take a zero-tolerance approach to sexual violence and sexual harassment.

Identify students who are involved in cybercrime, or those who are technically gifted and talented and are at risk of becoming involved in cybercrime and make a Cyber Choices referral.

Comply with the Xavier IT User Requirements.

Staff managing the technical environment will:

Provide technical support and perspective to the DSL, School Leadership team and Trustees, especially in the development and implementation of appropriate online safety policies and procedures, including all aspects of filtering and monitoring.

Be responsible for the technical implementation, maintenance and operation of filtering and monitoring systems.

Implement appropriate security measures as directed by the Leadership team to ensure that the school's IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.

Ensure the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges.

Ensure there is a clear, safe, and managed control of user access to networks and devices.

Ensure that our filtering policy and monitoring systems and approaches are effective and updated on a regular basis; responsibility for its implementation is shared with the leadership team.

Ensure filtering and monitoring systems and any other IT products comply with the Department for Education guidance '**Generative AI: product safety expectations 2026'.**

Conduct a cyber risk assessment annually and review every term. Create and implement a cyber awareness plan for students and staff. Complete actions required following concerns or checks to the system.

Secure digital technology and data with anti-malware and a firewall.

Control and secure user accounts and access privileges.

Licence digital technology and keep it up to date.

Develop and implement a plan to back up data and review annually.

Ensure regular filtering and monitoring reports are provided by Lightspeed to the DSL and Senior Leaders.

Report cyber-attacks both internally within the school or college and to external bodies.

Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL and/or deputies to enable them to take appropriate safeguarding action when required.

Ensure they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

Learners (at a level that is appropriate to their individual age and ability) will:

Engage in age/ability-appropriate online safety education.

Contribute to the development of online safety policies.

Read and adhere to the Xavier IT User Requirements and the Behaviour Policy.

Understand the importance of adopting safe and reasonable behaviours and online safety practices when using digital technologies outside of school and understand that the school's Xavier IT User Requirements also relates to actions outside of school, including on social media.

Respect the feelings and rights of others, on and offline.

Take an appropriate level of responsibility for keeping themselves and others safe online.

Understand the importance of reporting abuse, misuse or access to inappropriate materials. This includes using generative artificial intelligence (AI) responsibly, taking care not to generate or access inappropriate content.

Seek help from a trusted adult if they are concerned about anything they, or others, experience online.

Parents and carers will:

Read our Xavier IT User Requirements and encourage their children to adhere to them.

Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.

Role model safe and appropriate use of technology and social media.

Seek help and support from school or other appropriate agencies, if they or their child has any concerns with their use of technology.

Contribute to the development of our Online Safety policies.

Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies.

Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media; not sharing others' images or details without permission and refraining from posting negative, threatening or violent comments about others, including all members of the school community.

Education and engagement with learners

The school will establish and embed a whole-school safeguarding culture and will raise awareness and promote safe and responsible internet use amongst learners by:

- ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education and Computing programmes of study;
- reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site;
- teaching about the impact of technology on physical health, emotional wellbeing, sleep, relationships and learning;
- teaching learners how to identify online scams, fraud, financial exploitation, harmful online spending practices, gambling-related risks and manipulative features within games and online platforms;
- implementing appropriate peer education approaches through our Online Safety Student Group/School council;
- ensuring they understand the importance of reporting abuse, misuse or access to inappropriate materials, including incidents of sexual abuse and sexual harassment online;
- creating a safe environment in which all learners feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online;
- ensuring they know who to talk to if they have a concern.
- involving the DSL (or DDSL) as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any learners who may be impacted by the content;

- making informed decisions to ensure that any educational resources used are appropriate for our learners, including responsible use of generative artificial intelligence (AI);
- using external visitors, where appropriate, to complement and support our internal online safety education approaches;
- providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.
- seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

Insert name school will ensure learners develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:

- ensuring age-appropriate education regarding safe and responsible use precedes internet access;
- ensuring they understand the importance of adopting safe and responsible behaviours and good online safety practices when using digital technologies outside and realise that the school's Xavier IT User Requirements covers actions out of school, including on social media.
- informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- teaching learners to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable;
- educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation;
- enabling them to understand what acceptable and unacceptable online behaviour looks like;
- ensuring they understand the benefits/opportunities and risks/dangers of the online world and technology.
- preparing them to identify possible online risks and make informed decisions about how to act and respond;
- ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

Vulnerable Learners

Insert name school recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, some learners are more vulnerable online due to a range of factors, this may include, but is not limited to, looked-after children, children with special educational needs and disabilities (SEND) or mental health needs, and children experiencing trauma or loss.

Insert name school will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners.

Staff will seek input from specialist staff as appropriate, including the DSL, Deputy DSLs, SENDco, and Designated Teacher for Looked-after Children and IT Manager to ensure that the policy and curriculum is appropriate for all learners.

Training and engagement with staff

We will:

Provide and discuss the online safety policy and procedures with all members of staff as part of induction.

Provide up-to-date and appropriate online safety training, including the expectations, applicable roles and responsibilities in relation to filtering and monitoring, for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach. This will be part of our safeguarding and child protection training at induction for all staff and the training will be regularly updated. Staff training covers the potential risks posed to learners (content, contact, conduct and commerce) as well as our professional practice expectations.

Build on existing expertise by providing opportunities for staff to contribute to and shape our online safety approaches, including curriculum, policies and procedures.

Make staff aware that our IT systems are monitored, and that activity can be traced to individual users. Staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.

Make staff aware that their online conduct, including personal use of social media, can have an impact on their professional role and reputation.

Highlight useful educational resources and tools which staff could use with learners.

Ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving learners, colleagues or other members of the community.

Awareness and engagement with parents and carers

Insert name school recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to online safety with parents and carers by:

- providing information and guidance on online safety in a variety of formats. This will include highlighting online safety events such as parent evenings and transition events;
- drawing their attention to our online safety policy and expectations in our newsletters, on our website and other external communication;
- requesting parents and carers read online safety information when joining our community.

Reducing Online Risks

Insert name school recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

We will:

- regularly review the methods used to identify, assess and minimise online risks;
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use is permitted;
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material;
- recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and as such identify clear procedures to follow if breaches or concerns arise.
- Tailor teaching to emerging risks and the specific needs of our pupils.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence. This is clearly outlined in our Xavier IT User Requirements and highlighted through a variety of education and training approaches.

Safer Use of Technology

Classroom use

Insert Name of school uses a wide range of technology. This includes access to;

- Computers, laptops, tablets, mobile phones and other digital devices;
- Internet, which may include search engines and educational websites;
- Learning platform/intranet;
- Email;
- Digital cameras, web cams and video cameras.

All setting-owned devices will be used in accordance with our Xavier IT User Requirements and with appropriate safety and security measures in place.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending them for use at home.

The setting will use appropriate search tools as identified following an informed risk assessment:

- Google and Bing “SafeSearch” enforced by filtering policy;
- Suspicious search queries report generated weekly and emailed to the IT Manager and DSL for review;
- Staff to report inappropriate search results to the IT Manager and DSL.

We will ensure that the use of internet-derived materials, by staff and learners, complies with copyright law and acknowledge the source of information.

Supervision of internet access and technology use will be appropriate to learners' age and ability.

(Delete and amend Key stages as appropriate)

Early Years and Key Stage 1

Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners' age and ability.

Key Stage 2

Learners will use age-appropriate search engines and online tools.

Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners' age and ability.

Key Stage 3 and 4

Learners will use age-appropriate search engines and online tools.

Learners will be appropriately supervised during lessons when using technology, according to their ability and understanding.

Learners may have access to technology unsupervised, however appropriate levels of filtering and monitoring will be in place.

Key Stage 5

Learners will use age-appropriate search engines and online tools**.**

Learners will be able to use technology unsupervised, however appropriate levels of filtering and monitoring will be in place.

Managing internet access

We will maintain an online record of users who are granted access to our devices and systems.

All staff, learners and visitors will read and agree to Xavier IT User Requirements before being given access to our computer system, IT resources or the internet.

We will carry out regular audits and audit activity to help identify any users trying to access sites to establish vulnerabilities and offer support and advice and respond appropriately.

Filtering and monitoring

Leaders, managers and DSLs can access the guidance for education settings about establishing 'appropriate levels' of filtering and monitoring to help inform their decision making:

www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

Decision making

The Trust Board and school leaders have ensured that our school has age- and ability-appropriate filtering and monitoring in place to limit learner's exposure to online risks.

The school filtering and monitoring provision, agreed by senior leaders, governors and the IT Service Provider, is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Filtering and monitoring will be regularly reviewed and recorded, at least annually in line with the DfE Filtering and Monitoring Standards.

Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.

Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.

The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor.

The Trust Board and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

Day-to-day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety, and the IT service provider will have technical responsibility.

Appropriate filtering

Insert name school's education broadband connectivity is provided through *insert provider*.

Insert name school uses *insert provider* filtering system

Insert provider blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism,

drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.

Insert provider is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content.

Insert provider integrates 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'.

We work with *insert providers of broadband provider/filtering provider* to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.

Young learners will use child-friendly/age-appropriate search engines e.g SWGFL Swiggle.

If learners or staff discover unsuitable sites or material, they are required to turn off monitor/screen, report the concern immediately to a member of staff, report the URL of the site to technical staff/services.

Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate.

Parents/carers will be informed of filtering breaches involving their child.

Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.

Appropriate monitoring

We will appropriately monitor internet use on all setting-owned or provided internet-enabled devices. This may include:

- Physical monitoring (adult supervision in the classroom);
- Logging, monitoring and reviewing internet use;
- Review of insert name of monitoring software used e.g. lightspeed logs/reports;
- Reporting breaches to senior leaders;
- Use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring leads;
- Safeguarding software (*Insert name of software used*).

All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

If a concern is identified via monitoring processes, the IT Network Manager and DSL will respond in line with the child protection and safeguarding policy.

Managing personal data online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

Full information can be found in the Xavier Catholic Education Trust Data Protection Policy.

Security and management of information systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly;
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems;
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use;
- Not downloading unapproved software to work devices or opening unfamiliar email attachments;
- Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools;
- Checking files held on our network, as required and when deemed necessary by leadership staff;
- The appropriate use of user logins and passwords to access our network;
- Specific user logins and passwords will be enforced for all users;
- All users are expected to log off or lock their screens/devices if systems are unattended.

Password policy

- Password policy and procedures implemented are consistent with guidance from the National Cyber Security Centre.
- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- All learners have their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to
    - use strong passwords for access into our system;
    - change their passwords as instructed;
    - not share passwords or login information with others or leave passwords/login details where others can find them;
    - not to login as another user at any time;
    - lock access to devices/systems when not in use.

Managing the safety of our website

We will ensure that information posted on our website meets the requirements as identified by the DfE.

We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.

Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.

The administrator account for our website will be secured with an appropriately strong password.

We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

Publishing images and videos online

We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the Photography and Filming policy, Data Security, Xavier IT User Requirements and Code of Conduct.

Managing email

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including the Confidentiality Policy, Xavier IT User Requirements and the Code of Conduct.

The forwarding of any chain messages/emails is not permitted.

Spam or junk mail will be blocked and reported to the email provider.

Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

Setting email addresses and other official contact details will not be used to set up personal social media accounts.

Members of the community will immediately tell the DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.

Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

Staff email

All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted. The use of Xavier Catholic Education Trust email or school email for personal use is not permitted.

Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and parents.

Learner email

Learners will use a provided email account for educational purposes.

Learners will agree to the Xavier IT User Requirements and will receive education regarding safe and appropriate email use before access is permitted.

Whole-class or group email addresses will be used for communication outside of the setting other than when providing feedback on work completed.

Management of learning platforms

Insert name school uses *insert provider* as an official learning platform.
Leaders and staff will regularly monitor the usage of the Learning Platform, including message/communication tools and publishing facilities.

Only current members of staff, learners and parents will have access to the Learning Platform. When staff and/or learners leave the setting, their account will be disabled.

Parents and staff will be advised about acceptable conduct and use when using the Learning Platform.

All users will be mindful of copyright and will only upload appropriate content onto the Learning Platform.

Any concerns about content on the Learning Platform will be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive;
- If the user does not comply, the material will be removed by the site administrator;
- Access to the Learning Platform for the user may be suspended;
- The user will need to discuss the issues with a member of leadership before reinstatement;
- If the content is illegal, we will respond in line with existing child protection procedures.

A visitor may be invited onto the Learning Platform by a member of the leadership team as part of an agreed focus or a limited time slot.

Management of applications (apps) used to record children's progress

We use *insert provider* to track learners' progress and share appropriate information with parents and carers.

The Headteacher will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

To safeguard learners' data:

- only school-issued devices will be used for apps that record and store learners' personal details, attainment or photographs;
- personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images;
- devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft;
- all users will be advised regarding safety measures, such as using strong passwords and logging out of systems;
- parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

Use of Social Media

Expectations

The expectations regarding safe and responsible use of social media applies to all members of the school community.

The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger apps or other online communication services.

All members of the school community are expected to engage in social media in a positive and responsible manner.

All members of the school community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

We will control learner and staff access to social media whilst using school-provided devices and systems on site.

- The use of social media during school hours for personal use is not permitted for staff;
- The use of social media during school hours for personal use is not permitted for learners;
- The use of social media sites is restricted to the Headteacher and Business Manager by filtering policy;
- Inappropriate or excessive use of social media during school hours or whilst using school devices may result in removal of internet access and/or disciplinary or legal action.

Add/delete as appropriate for the school.

The use of social media or apps, for example as a formal remote learning platform, will be risk assessed by the DSL and/or Headteacher prior to use. Any use will take place in accordance with our Xavier IT User Requirements.

Concerns regarding the online conduct of any member of the school community on social media will be taken seriously. Concerns will be managed in accordance with our Child Protection and Safeguarding policy and Code of Conduct and Managing Allegations policies.

Staff use of social media

The use of social media during school hours for personal use is/is not permitted for staff. (amend as appropriate for the school) If it is permitted, it should state when or whether it is with explicit permission.

The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff on a regular basis.

Safe and professional behaviour will be outlined for all members of staff, including volunteers, as part of our Code of Conduct, Xavier IT User Requirements and Child Protection and Safeguarding policy.

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school

Disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
All members of staff are advised to safeguard themselves and their privacy when using social media services. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include, but is not limited to:

- Setting appropriate privacy levels on their personal accounts/sites;
- Being aware of the implications of using location sharing services;
- Opting out of public listings on social networking sites;
- Logging out of accounts after use;
- Using strong passwords;
- Ensuring staff do not represent their personal views as being those of the school.

All members of staff are encouraged to carefully consider the information, including text and images they share and post online. Staff are expected to ensure that their social media use is compatible with their professional role and is in accordance with our policies, and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues, will not be shared or discussed on social media sites.

Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents/carers

Staff will not use personal social media accounts to contact learners or parents/carers, nor should any contact be accepted.

All members of staff are advised not to communicate with or add any current or past learners or their family members, as 'friends' on any personal social media sites, applications or profiles.

Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the Headteacher.

Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the setting and members of staff.

If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks, or to use official, setting-provided communication tools.

Any communication from learners and parents received on personal social media accounts will be reported to the DSL and the Headteacher.

Learners' use of social media

Insert name of school will empower learners to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks and know to share any concerns with a trusted adult. Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources.

We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for learners under the required age as outlined in the services terms and conditions.

Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including the Behaviour policy and Child Protection and Safeguarding policy.

The DSL or DDSL will respond to social media concerns involving Safeguarding or Child Protection risks in line with our Child Protection and Safeguarding policy.

Sanction and/or support will be implemented and offered to learners as appropriate, in line with our Child Protection and Safeguarding policy. Civil or legal action may be taken if necessary.

Concerns regarding learners' use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

Learners will be advised:

- to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location;
- to only approve and invite known friends on social media sites and to deny access to others by making profiles private;
- not to meet any online friends without a parent/carer or other appropriate adult's permission, and to only do so when a trusted adult is present;
- to use safe passwords;
- to use social media sites which are appropriate for their age and abilities;
- how to block and report unwanted communications;
- how to report concerns on social media, both within the setting and externally.

Official use of social media

Insert name of school official social media channels are:

- X (formerly known as Twitter) and insert name of any other social media channels used

The official use of social media sites by *insert name of school* only takes place with clear educational or community-engagement objectives and with specific intended outcomes and the use has been formally risk assessed and approved by the Headteacher.

Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.

Staff use setting-provided email addresses to register for and manage official social media channels.

Official social media sites are suitably protected and, where possible, run and are linked to our website.

Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

Official social media use will be conducted in line with existing policies, including but not limited to Behaviour, Photography and Filming, Data Protection, Child Protection and Safeguarding and Code of Conduct.

All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.

Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

Any official social media activity involving learners will be moderated if possible.
Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.

We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional accounts where possible, to avoid blurring professional boundaries.

If members of staff are managing and/or participating in online social media activity as part of their capacity as an employee of the setting, they will:

- Read, understand and adhere to the Xavier IT User Requirements;
- Be aware they are an ambassador for the setting;
- Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared;
- Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws;
- Follow our Photography and Filming policy at all times and ensure appropriate consent has been given before sharing images on the official social media channel;
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so;
- Not engage with any private/direct messaging with current or past learners or parents/carers;
- Inform their line manager, the DSL and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

Mobile Technology: Use of Personal Devices and Mobile Phones

Insert name of school recognises that personal communication through mobile technologies is part of everyday life for many learners, staff and parents/carers. Mobile technology needs to be used safely and appropriately within the school.

Expectations

All use of mobile technology, including mobile phones and personal devices such as tablets, games consoles and wearable technology will take place in accordance with our policies, such as the Behaviour policy and Child Protection and Safeguarding policy, and with the law.

All users of mobile technology devices should understand that the primary purpose of the use of mobile/personal devices in a school context is educational.

Electronic devices of any kind that are brought onto site are the responsibility of the user.

- Pupils are not permitted to bring smartphones or other smart devices to school. If a phone is required for travel, it must be a basic phone (no internet access) and handed in at the start of the day. There may be some pupils who require a smartphone for the management of medical needs e.g. diabetes. Individual cases should be discussed with the Headteacher.
- All members of *insert name of school* community are advised to take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- All members of *insert name of school* community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms, toilets and classrooms. Staff should only use their personal mobile phone in the staff room or outside the school premises where pupils are not present.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our Behaviour policy and Code of Conduct.

All members of *insert name of school* community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory, or illegal, or would otherwise contravene our Behaviour or Child Protection and Safeguarding policies.

Staff use of personal devices and mobile phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as relevant policy and procedures, such as Confidentiality, Child Protection and Safeguarding, Data Security and Xavier IT User Requirements.

Staff will be advised to

- keep mobile phones and personal devices in a safe and secure place e.g. locked in a locker/drawer or cupboard during lesson time;
- keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times;
- ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times;
- not use personal devices during teaching periods, unless written permission has been given by the Headteacher such as in emergency circumstances;
- ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and our behaviour expectations.

Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.

- Any pre-existing relationships which could undermine this will be discussed with the DSL and Headteacher.

Staff will not use personal devices or mobile phones:

- to take photos or videos of learners and will only use work-provided equipment for this purpose;
- directly with learners and will only use work-provided equipment during lessons/educational activities;
- to communicate with parents/carers.

Where remote learning activities take place, staff will use equipment provided by school. If this is not available, staff will only use personal devices with prior approval from the Headteacher, following a risk assessment. Staff will follow clear guidance set out in the Acceptable Use of Technology policy.

If a member of staff breaches our policy, action will be taken in line with our Code of Conduct, Child Protection and Safeguarding policy and Managing Allegations policy.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our Child Protection and Safeguarding policy and Managing Allegations policy.

Learners' use of personal devices and mobile phones

Learners will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices and will be made aware of behaviour expectations and consequences for policy breaches. Personal devices include any other electronic devices with imaging and sharing capabilities.

Safe and appropriate use of mobile phones and smart technology will be taught to learners as part of an embedded and progressive safeguarding education approach, using age-appropriate sites and resources.

Mobile phones and/or personal devices will/will not be used on site by learners (amend as appropriate and include any specific requirements if they are allowed)

Insert name of school expects learners' personal devices and mobile phones to be kept in a secure place during the school day.

If a learner needs to contact their parents or carers they will be allowed to use the school phone.

Parents are advised to contact their child via the school office. Exceptions may be permitted on a case-by-case basis, as approved by the Headteacher.

If a learner requires access to a personal device in exceptional circumstances, for example medical assistance, this will be discussed with the Headteacher prior to use being permitted.

Where learners' mobile phones or personal devices are used when learning at home, this will be in accordance with our Acceptable Use of Technology policy.

Mobile phones and personal devices must not be taken into examinations. Learners found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body.

Mobile phones or personal devices will not be routinely used by learners during lessons or formal educational time.

The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.

Any concerns regarding learners' use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including Behaviour and Child Protection and Safeguarding.

- Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene the Child Protection and Safeguarding or Behaviour policy.
- Searches of mobile phone or personal devices will be carried out in accordance with '*Searching, Screening and Confiscation'* guidance.
- Learners' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/carer. Content may be deleted or requested to be deleted, if it contravenes our policies, in line with the DfE '*Searching, Screening and Confiscation'* guidance.
- Mobile phones and devices that have been confiscated will be held in a secure place and released to parents/carers at the end of the school day or week.
- Appropriate sanctions and support will be implemented in accordance with our behaviour policy.

- Concerns regarding policy breaches by learners will be shared with parents/carers as appropriate.
- Where there is a concern that a child is at risk of harm, we will respond in line with our Child Protection and Safeguarding policy.
- If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Visitors' use of personal devices and mobile phones

Parents/carers and visitors, including volunteers and contractors, will be informed that mobile phones are only permitted within specific areas of the school.

Information is provided at signing in to inform parents/carers and visitors of expectations of use.

Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our Acceptable Use policy and other associated policies, including but not limited to Behaviour, Child Protection and Safeguarding and Photography and Filming.

Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology (including any personal electronic device with camera or image recording capabilities) and will inform the DSL or Headteacher of any breaches of our policy.

Officially provided mobile phones and devices

Members of staff will be issued with a work phone number and email address, where contact with learners or parents/carers is required. (Amend as appropriate.)

School mobile phones will be suitably protected via a passcode/password or PIN and must only be accessed or used by members of staff and/or learners who have permission to use them.

School mobile phones and devices will always be used in accordance with the Acceptable Use of Technology policy and other relevant policies. School mobile phones and/or devices may be monitored for safeguarding reasons and to ensure policy compliance.

Responding to Online Safety Incidents and Concerns

All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, child-on-child abuse, including cyberbullying and making and sharing of nudes and semi nudes, including AI generated inappropriate content, online sexual violence and harassment, online abuse and exploitation and illegal or inappropriate content. This includes: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

All members of the community will be made aware of the availability of the Cyber Choices early intervention programme for individuals who are involved in cybercrime, or those with a particular skill and interest in computing and technology who may be at risk of becoming involved in cybercrime.

All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.

Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents, carers and learners to work in partnership with us to resolve online safety issues.

After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

If we are unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Service and/or C-SPA.

Where there is a concern that illegal activity has taken place, we will follow the SSCP procedures which will include contacting the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.

If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the Headteacher will speak with the police and the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.

Concerns about learner online behaviour and/or welfare

The DSL will be informed of all online safety concerns involving safeguarding or child protection risks in line with our Child Protection and Safeguarding policy.

All concerns will be recorded in line with our Child Protection and Safeguarding policy.

Insert name of school recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse other children; all online child-on-child abuse concerns will be responded to in line with our Child Protection and Safeguarding and Behaviour policies.

The DSL will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.

Appropriate sanctions and/or pastoral/welfare support will be offered to learners as appropriate.

We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

Concerns about staff online behaviour and/or welfare

Any complaint about staff misuse will be referred to the Headteacher in accordance with our Child Protection and Safeguarding policy and Code of Conduct.

Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

All low-level concerns regarding a member of staff's online conduct will be managed in accordance with the Child Protection and Safeguarding policy and Allegations and low-level concerns raised in relation to staff, supply staff, contractors and volunteers' policy.

Appropriate action will be taken in accordance with our Code of Conduct.

Welfare support will be offered to staff as appropriate.

Concerns about parent/carer online behaviour and/or welfare

Concerns regarding parents'/carers' behaviour and/or welfare online will be reported to the headteacher. The headteacher will respond to concerns in line with existing policies, including but not limited to Child Protection and Safeguarding, Complaints, Code of Conduct, Acceptable Use and Behaviour policy.

Appropriate action will be taken, if necessary, in line with Child Protection and Safeguarding policy and the staff Code of Conduct.

Welfare support will be offered to parents/carers as appropriate.

Procedures for Responding to Specific Online Incidents or Concerns

Online sexual violence and sexual harassment between children

Our Headteacher, DSL and appropriate members of staff have accessed and understood part 5 of Keeping Children Safe in Education 2026.

- Full details of our response to child-on-child abuse, including sexual violence and harassment, can be found in our Child Protection and Safeguarding policy.

Insert name of school recognises that sexual violence and sexual harassment between children can take place online. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include;

- Consensual and non-consensual sharing of nudes and semi-nudes' images and/or videos;

- Sharing of unwanted explicit content;
- Sexualised online bullying;
- Unwanted comments and messages, including on social media;
- Sexual exploitation; coercion and threats, and
- Coercing others into sharing images of themselves or performing acts they're not comfortable with online.

We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

We recognise that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

We recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

To help minimise concerns, will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment by implementing a range of age- and ability-appropriate educational methods as part of our curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

If made aware of any concerns relating to online sexual violence and sexual harassment, we will:

- immediately notify the DSL and act in accordance with our Child Protection and Safeguarding and Behaviour policies;
- manage the learners' personal devices in accordance with the DfE 'searching screening and confiscation' advice, where the content is contained on learners' personal devices.
- provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support;
- implement appropriate sanctions in accordance with our Behaviour Policy;
- inform parents and carers, if appropriate, about the incident and how it is being managed;
- If appropriate, make referrals to partner agencies, such as Children's Services and/or the police;
- If the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community;
- If a criminal offence has been committed, the DSL will discuss this with the police first to ensure that investigations are not compromised;
- review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Sharing Nudes and Semi-Nude Images and/or Videos (also known as Youth produced sexual imagery or Sexting)

Insert name of school recognises Sharing Nudes and Semi Nudes Images and/or Videos as a safeguarding issue; all concerns will be reported to and dealt with by the DSL.

We will follow the advice as set out in the non-statutory UK Council for Internet Safety (UKCIS) guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk).

Sharing Nudes/Semi-Nudes refers to both images and videos where:

- A person under the age of 18 creates and shares sexual imagery of themselves with another child under the age of 18;
- A person under the age of 18 shares sexual imagery created by another child under the age of 18 with a child under the age of 18 or an adult;
- A person under the age of 18 is in possession of sexual imagery created by another person under the age of 18.

It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.

We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth-produced sexual imagery by implementing preventative approaches, via a range of age- and ability-appropriate educational methods.

We will ensure that all members of the community are aware of sources of support regarding the making and sharing of nudes and semi nudes, including AI generated inappropriate content.
We will respond to concerns regarding nudes and semi-nude images, regardless of whether the incident took place on site or using setting-provided or personal equipment.

We will not:

- view any images suspected of being youth-produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so. If it is deemed necessary, the imagery will only be viewed where possible by the DSL, and any decision making will be clearly documented.
- send, share, save or make copies of content suspected to be an indecent image/video of a child (i.e. nudes and semi nudes) and will not allow or request learners to do so.
- Delete the imagery or ask the young person to delete it.
- Ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- Share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- Say or do anything to blame or shame any young people involved.

If made aware of an incident involving the creation or distribution of youth-produced sexual imagery, we will:

- act in accordance with our Child Protection policies and the relevant local procedures.
- ensure the DSL responds in line with the UKCIS and SSCP guidance.
- store any devices containing potential nude or semi-nude images securely.
- If content is contained on learners' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- If a potentially indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- carry out a risk and needs assessment in line with the UKCIS and SSCP guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies.
- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
- make a referral to Children's Services and/or the police, as deemed appropriate in line with the UKCIS and SSCP guidance.
- provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- implement appropriate sanctions in accordance with our Behaviour policy but taking care not to further traumatise victims where possible.
- consider the deletion of images in accordance with the UKCIS guidance. Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved and are sure that to do so would not place a child at risk or compromise an investigation.
- review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

Insert name of school recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL, in line with our Child Protection and Safeguarding policy.

We will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target learners, and understand how to respond to concerns.

We will implement preventative approaches for online child abuse and exploitation via a range of age- and ability-appropriate education for learners, staff and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.

We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community.

If made aware of an incident involving online child abuse and/or exploitation, we will:

- act in accordance with our Child Protection and Safeguarding policy and the relevant SSCP procedures.
- store any devices containing evidence securely.
    - If content is contained on learners' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
- If appropriate, make a referral to Children's Services and inform the police via 101, or 999 if a learner is at immediate risk.
- carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies.
- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
- provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
- review the handling of any incidents to ensure that best practice is implemented; Leadership team will review and update any management procedures, where necessary.
  We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using setting-provided or personal equipment.
- Where possible and appropriate, learners will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: www.ceop.police.uk/safety-centre/ .

If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Education Safeguarding Service and/or police.

If made aware of intelligence or information which may relate to child exploitation (on or offline), it will be passed through to the police by the DSL.

If members of the public or learners at other settings are believed to have been targeted, the DSL will seek advice from the police, C-SPA and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

Indecent Images of Children

Insert name of school will ensure that all members of the community are made aware of the possible consequences of accessing indecent images of children.

We will respond to concerns regarding indecent images of children on our equipment and/or personal equipment, even if access took place off site.

We will seek to prevent accidental access to indecent images of children by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.

If we are unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the police and/or the Education Safeguarding Service.

If made aware of indecent images of children, we will:

- act in accordance with our Child Protection and Safeguarding policy and the relevant Surrey Safeguarding Children Partnership procedures.
- store any devices involved securely.
- immediately inform appropriate organisations, such as the IWF, police and LADO.

If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:

- ensure that the DSL is informed.
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
- ensure that any copies that exist of the image, for example in emails, are deleted.
- report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting-provided devices, we will:

- ensure that the DSL is informed.
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
- ensure that any copies that exist of the image, for example in emails, are deleted.
- inform the police via 101 or 999 if there is an immediate risk of harm, and Children's Services, as appropriate.
- only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
- report concerns, as appropriate to parents/carers.

If made aware that a member of staff is in possession of indecent images of children on school-provided devices, we will:

- ensure that the Headteacher is informed in line with our Child Protection and Safeguarding policy and Managing Allegations policy immediately and without delay.
- inform the LADO and other relevant organisations in accordance with our Child Protection and Safeguarding policy and Managing Allegations policy.
- quarantine any devices until police advice has been sought.

Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at insert name of school and full details of how we will respond to cyberbullying are set out in our Behaviour policy and Anti-bullying policy.

Online hate

Online hate content directed towards or posted by specific members of the community will not be tolerated and will be responded to in line with existing policies, including Child Protection and Safeguarding, Anti-bullying and Behaviour.
All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

The police will be contacted if a criminal offence is suspected.

If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Education Safeguarding Service and/or the police.

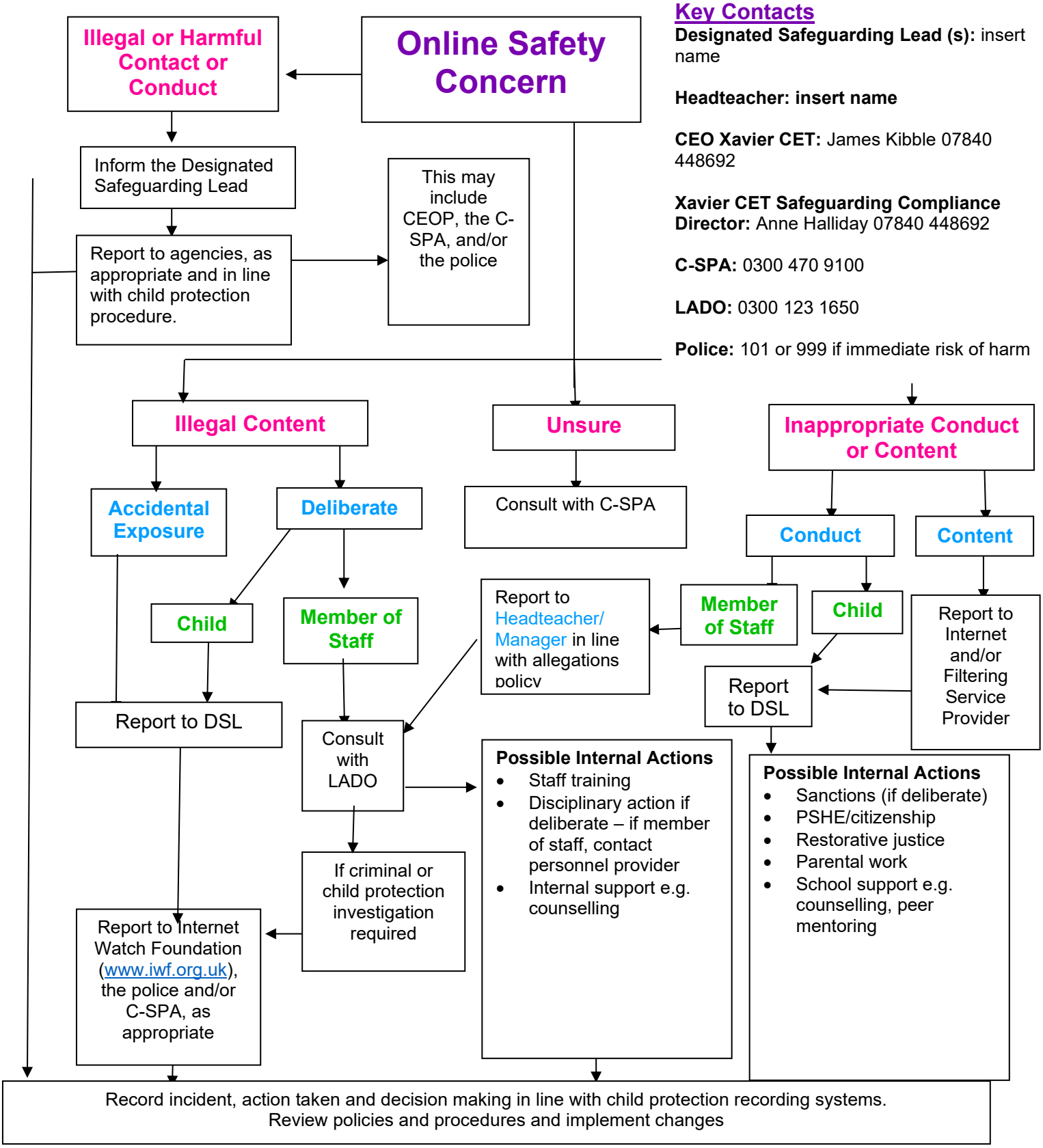
Online radicalisation and extremism

As referenced in this policy, we will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.

If we are concerned that a learner or adult may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our Child Protection and Safeguarding policy and Surrey Prevent referral process.

If we are concerned that a member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the Child Protection and Safeguarding policy and Managing Allegations policy.

Responding to an Online Safety Concern Flowchart



Key Contacts

Designated Safeguarding Lead (s): insert name

Headteacher: insert name

CEO Xavier CET: James Kibble 07840 448692

Xavier CET Safeguarding Compliance Director: Anne Halliday 07840 448692

C-SPA: 0300 470 9100

LADO: 0300 123 1650

Police: 101 or 999 if immediate risk of harm

Useful Links

Surrey Safeguarding Children's Partnership: https://www.surreyscp.org.uk/

Surrey Education Safeguarding Team 01483 517008

Surrey Police:
Surrey Police
In an emergency (a life is in danger or a crime in progress) dial 999. For non-urgent enquiries, contact Surrey Police via 101

C-SPA:

- 0300 470 9100 (Mon-Fri 9am-5pm)
- 01483 517898 (Out of hours emergency duty team)

National Links and Resources for Schools, Learners and Parents/Carers

Reporting Harmful Content

IWF Internet Watch Foundation https://www.iwf.org.uk/

REPORT HARMFUL CONTENT https://reportharmfulcontent.com/

CEOP A National Crime Agency command https://ceop.police.uk/safety-centre/

Websites to visit for online safety information:

THINK U KNOW Thinkuknow: Parents and Carers: https://www.ceopeducation.co.uk/parents/

Thinkuknow Parents and Carers is an education programme developed by The National Crimes Agency's Child Exploitation and Online Protection Centre (CEOP). It offers parents advice on a range of issues relating to children's safety and wellbeing within a digital world.

NSPCC: www.nspcc.org.uk/onlinesafety

Resources produced by the NSPCC to stay safe online as a family. They provide advice on inappropriate and sexual behaviour online, online gaming and parental controls. The NSPCC helpline number is 0808 8005002

ChildLine: www.childline.org.uk

Sexting and sending nudes | Childline

The ChildLine website provides information and advice on a wide range of issues including online and offline safety. Advice includes using social media, cyberbullying, online grooming, taking care of your digital footprint and mobile phone safety. Childline also provides guidance to help young people decline requests for nudes and inappropriate content and how to ask for the message to be deleted. The ChildLine helpline is 0800 1111

UK Safer Internet Centre: www.saferinternet.org.uk

UK Safer Internet Centre provides online safety tips, advice and resources to help children and young people stay safe online. Advice also includes setting up parental controls and what to consider before buying mobile devices.

Childnet: www.childnet.com

Childnet has resources, including videos and storybooks, to help you discuss online safety with your children. It includes advice on setting up parental controls, cyberbullying and setting up a family agreement for safer internet use. It has a parent and carer toolkit. Childnet have produced smart rules for online safety, using Widget symbols; these can be displayed near computers as a visual reminder. They have also produced the STAR SEN Toolkit to explore online safety with young people who have special educational needs.

www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals

Guidance and training resources developed to provide professionals, who work with young people, with practical tips and advice on understanding, preventing and responding to online sexual harassment in educational settings.

Internet Matters: www.internetmatters.org

Internet Matters provides advice by age group. Advice incudes setting up appropriate controls and filters on a range of devices, cyberbullying, online grooming and self-harm.

https://www.internetmatters.org/resources/theonlinetogetherproject/tackling-online-hate-quiz/

Empower young people to tackle online hate and challenge negative behaviours in their digital spaces with this interactive tool.

Parent Zone: https://parentzone.org.uk/

Parent Zone is a parenting organisation working to make the online world a safer, more positive place for families and children. Explore the ways Parent Zone can help your family, school or organisation understand online safety.

BBC online safety resources for primary schools: Primary online safety for teachers

Each of these collections have been mapped to the Education for a Connected World framework set out by the UK Council for Internet Safety. Pages contain downloadable teacher resource documents with lesson ideas, discussion points and potential homework activities.

360 Safe: https://360safe.org.uk/

LGfL: https://lgfl.net/TypesOfHarm/OnlineSafetyAudit

A free online safety self-review tool for schools can be found via the 360 safe website or LGfL online safety audit.