St Leonard's Church of England Primary School

Online Safety Policy

Date written & reviewed :	12.05.24
Policy written by:	Miss Kealey
Date of next review:	May 2025

In Jesus' Footsteps, we will grow in grace and knowledge.

St Leonard’s School Online Safety Policy

Introduction to Online Safety

New technologies have become integral to the lives of children and young people in today’s society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

The requirement to ensure that children are able to use online and related communications technologies appropriately and safely is addressed as part of the wider duty of care, to which all who work in schools are bound. The school Online Safety Policy and procedures will help to ensure safe and appropriate use. The development and implementation of such a strategy will involve all the stakeholders in a child’s education from the Head teacher and Governors to the senior leaders, classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

As with all other risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision to build pupils’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with them.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything, reasonably expected of them, to manage and reduce these risks.

The Online Safety Policy and procedures that follows, explains how we intend to do this. While also addressing wider educational issues, in order to help young people (and their parents) to be responsible users and stay safe, when using the internet and other communication technologies for educational, personal and recreational use.

Policy Aims (Intent)

The school and governing body, incorporating Government and Local Authority guidance, have developed this policy. It takes into account the Department for Education statutory guidance; ‘Keeping Children Safe in Education’ 2024, Early Years and Foundation Stage 2024 , ‘Working Together to Safeguard Children’ 2023.

The purpose of the school’s online safety policy is to:

- Set out the key principles expected of all members of the school community at St Leonard’s Church of England Primary School with respect to the use of Internet based technologies
- Safeguard and protect all members of St Leonard’s School community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff, working with children, 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 use when responding to online safety concerns.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross-referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

St Leonard’s School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Policy Scope

- St Leonard’s School believes 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.
- St Leonard’s School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- St Leonard’s School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support 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, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, iPads, Chromebooks or mobile phones.

Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Safeguarding and Child Protection policy
- Anti-Bullying policy
- Code of Conduct policy
- Behaviour policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Privacy policy - Data Protection (GDPR)

Monitoring and Review

- Technology in this area evolves and changes rapidly. St Leonard’s School will review this policy at least annually.
- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- 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 a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

Roles and Responsibilities

Governors

The role of the Governors/Online Safety Governor is to:

- Ensure that the school follows all current online safety advice to keep the children and staff safe;
- Approve the Online Safety Policy and procedures and review its effectiveness.
- Support the school in encouraging parents and the wider community to become engaged in online
  safety activities;
- Regular review with the Headteacher to discuss incident logs, Netsweeper
- filtering logs
- Access appropriate and up-to-date online safety training.

Headteacher

Reporting to the governing body, the Headteacher/DSL (Designated Safeguarding Lead) Mrs Lindley, has overall responsibility for online safety within school.

The Headteacher will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Access regular, appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant up to date knowledge required to keep learners safe online.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training
- Maintain records of online safety concerns, as well as actions taken, as part of the school safeguarding recording mechanisms.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident occurring.
- Receive regular weekly monitoring log reports from Netsweeper filter.
- Be aware of the procedures to be followed in the event of a serious online safety incident or an allegation being made against a pupil, member of staff or volunteer.

Computing Lead

They will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies / documents
- Provide training and advice for staff.

- Advise the Head teacher and governing body on all online safety matters.
- Report online safety concerns, as appropriate, to the Headteacher/DSL.
- Collaborate with the PSHE/RSE lead and school's senior management team to ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety. Mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression.
- Engage with parents and the school community on online safety matters at school and/or at home via newsletters, school website.
- Liaise with our technical support providers, Western Business Systems (school server and wireless systems) and Vitalize IT (Chromebook management).
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Monitor school network/internet use via weekly Netsweeper filtering reports in order that any attempted misuse is reported to the Headteacher.

Teachers and Support Staff

It is the responsibility of all members of staff to:

- Read, understand and help promote the school's Online Safety Policy and procedures.
- Read, understood and adhere to the school Staff Acceptable Use Agreement.
- Be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school procedures with regard to these devices;
- Report any suspected misuse or problem to the Computing lead and /or Headteacher.
- Identify online safety concerns and take appropriate action by following the school safeguarding policies and procedures.
- Maintain an awareness of current online safety issues and guidance e.g. through CPD opportunities;
- Model safe, responsible and professional behaviours in their own use of technology;
- Ensure that any digital communications with pupils are on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones or social media messaging or posts.

Teachers must:

- Ensure that online safety issues are embedded in all aspects of the curriculum and other school activities.
- Monitor, supervise and guide pupils carefully when engaged in ICT activity in lessons, extra-curricular and extended school activities.
- Ensure that pupils are fully aware of research skills and are made aware of legal issues relating to electronic content such as copyright laws.

- Ensure that during lessons where internet use is pre-planned pupils are guided to sites checked as suitable for their use and that processes are known and used when dealing with any unsuitable material that is found in internet searches.
- Ensure pupils understand and follow the Online Safety and Acceptable Use Agreement.

Pupils

Taking into account the age and level of understanding, the key responsibilities of pupils are to:

- Use the school ICT systems in accordance with the Pupil Acceptable Use Agreement which they and/or their parents will be expected to sign before being given access to school systems
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Know and understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology;
- Know and understand school procedures on the use of mobile phones, digital cameras and hand-held devices.
- Know and understand school procedures on the taking/use of images and on cyber-bullying;
- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy and procedures covers their actions out of school, if related to their membership of the school;
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.
- Help the school in the creation/review of the Online Safety Policy and procedures.

Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents do not fully understand the issues and are less experienced in the use of ICT than their children are. The school will take every opportunity to help parents understand these issues through newsletters, school website and information about national/local online safety campaigns/literature.

The key responsibilities for parents are to:

- Read the acceptable use policies 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.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Technical Support Provider

Technical support for the maintenance of our school systems and infrastructure is outsourced to Western Business Systems.
Their responsibilities are to ensure:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations etc from accidental or malicious attempts, which might threaten the security of the school systems and data.
- The school server, workstations and laptops are protected by Sophos Antivirus software that automatically updates.
- All users have clearly defined access rights to school technical systems and devices through group policies so that only the relevant group of users can access a resource.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- Servers, wireless systems and cabling will be securely located and physical access restricted
- Internet filtering ensures that children are safe from terrorist and extremist material when accessing the internet.
- Appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster and in order to complement the business continuity process

Training

Staff and Governor Training

St Leonard’s will;

- Ensure staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.
- Make regular training available to staff on online safety issues and the school’s online safety education programme
- Provide, as part of the induction process, all new staff (including those on university/college placements and work experience) and volunteers with information and

guidance on the Online Safety Policy, procedures and the school's Acceptable Use Agreements.

Parent Awareness and Training

St Leonard's 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:

- The introduction of the school's Acceptable Use Agreements to new parents, to ensure that our principles of online safety behaviour are made clear.
- Providing information and guidance on online safety via a dedicated web page on the school website, newsletters and emails.
- Curriculum activities.
- High profile events/campaigns e.g. Safer Internet Day

Teaching and Learning

Why Internet use is Important

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

How Internet Use Benefits Education

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries.
- Inclusion in the National Education Network (NEN) which connects all UK schools
- Educational and cultural exchanges between pupils worldwide.
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.

- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administration data with the Local Authority and DfE.
- Access to learning wherever and whenever convenient.

How Internet Use Enhances Learning

St Leonard's has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE curriculum. This covers the teaching of a range of skills and behaviours that are appropriate to the age and experience of the pupils concerned and include those to:

- Develop a range of strategies to evaluate and verify information before accepting its accuracy;
- Be aware that the author of a website/page may have a bias or purpose and to develop skills to recognise what that may be.
- Know how to narrow down or refine a search.
- [for older pupils] Understand how search engines work and to understand that this affects the results they see at the top of the listings.
- Understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- Understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- Understand why they should not post or share detailed accounts of their personal lives; contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- Understand why they must not post pictures or videos of others without their permission;
- Know not to download any files – such as music files – without permission.
- Have strategies for dealing with receipt of inappropriate materials.
- [for older pupils] Understand why and how some people will 'groom' young people for sexual reasons.
- Understand the impact of cyberbullying, sexting and trolling and know how to seek help if any form of online bullying affects them.
- Know how to report any abuse including cyberbullying and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- Plan Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind pupils about their responsibilities through an end-user Acceptable Use Agreement which will be displayed throughout the school.
- Ensure staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensure that when copying materials from the web, staff and pupils understand issues around plagiarism. How to check copyright and know that they must respect and acknowledge copyright/intellectual property rights.

- Ensure that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. These may include risks from pop-ups, buying online, online gaming/gambling etc.
- Support pupils in building resilience to radicalisation by providing a safe environment for debating issues and help them to understand how they can influence and participate in decision-making.

Pupils with Additional Needs

For children who may require additional support to move forward in safeguarding themselves the school may implement the following strategies:

- Additional teaching that includes reminders and explicit prompts to link their existing knowledge of “how to keep safe” to the rules that will apply specifically to, for instance, internet use.
- Consider that some pupils who will usually learn rules within certain contexts, but who will find it difficult to transfer these rules across environments, lessons or teachers.
- Establish online safety rules for school that are similar to those for home. Working with parents and sharing information with them would be relevant to all children, but this group especially.
- Visual support is usually important to help most pupils’ understanding but some areas of this topic are quite abstract in nature and difficult to represent visually i.e.
    - o Uncomfortable
    - o Smart
    - o Stranger
    - o Friend
- Some pupils are very quick to click with the mouse and may not actually know what they did or how something happened. Gentle investigation will be more productive than asking many questions.
- Some pupils may not be able to ask for help. Staff will need to know specific pupils well so that this can be addressed.

Reducing Online Risks

St Leonard’s 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 use in school 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.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.

- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online. The importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the school community. These are clearly outlined, in our acceptable use policies, and highlighted through a variety of education and training approaches.

Safer Use of Technology

Classroom Use

St Leonard's School uses a wide range of technology including access to:

- Computers, laptops and other digital devices (eg. iPads, Chromeboooks)
- Internet which may include search engines and educational websites
- Email
- Digital cameras, web cams and video cameras
- School servers and wifi system.

All school owned devices will be used in accordance with our acceptable use policies 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 for use at home.
- The school will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community

Filtering

St Leonard's School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.

- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regard to online activities and safeguarding.
- 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.

Lancashire County Council's Education Digital Services (EDS), provide education broadband connectivity at St Leonard's through the CLEO network (covering Cumbria and Lancashire) to connect to the internet through the UK Universities (JANET) network. JANET also interconnects with other regional schools' networks across the UK to form The National Education Network (The NEN).

Netsweeper (selected by EDS) provide internet filtering to connected schools, including St Leonard's.

It provides:

- Enhanced SSL Filtering as standard
- A filtering system which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature
- Excellent reporting facilities and a secure dual site configuration

It is also compliant with the UK Safer Internet Centre guidance. Netsweeper's completed checklist on UK Safer Internet Centre site accessed via the link below. This document illustrates how Netsweeper filtering meets the national defined ‘appropriate filtering standards'.

If pupils discover unsuitable sites, they will be required to:

- Turn off the monitor and report their concern immediately to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the Headteacher/ DSL (or deputy) and/or Computing lead.
- The breach will be recorded and reported to Lancashire County Council Education Digital Services and Netsweeper.
- Parents/carers will be informed of filtering breaches involving their child.

Monitoring

All users, staff/pupils/visitors 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.
The school IT systems will be monitored as follows:

- The Headteacher (DSL) receives weekly reports from Netsweeper detailing online traffic over the school systems.

- Online safety incidents being documented and reported immediately to the Headteacher (DSL) and Computing lead who will arrange for these to be dealt with immediately, in accordance with school policies

Managing Personal Data Online

Personal data is recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
Full information can be found in our Privacy policy, which is published on our school website.

Staff must ensure that they:

- At all times, take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password-protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Disposal of Redundant ICT Equipment

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment, that may have held personal data, will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to:
  - The Waste Electrical and Electronic Equipment Regulations 2006
  - The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
  - Environment Agency Guidance (WEEE) Click here to access
  - ICO Guidance - Data Protection Act 1998 Click here to access
  - Electricity at Work Regulations 1989
- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

Security and Management of Information Systems

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

- Virus protection updated automatically.
- 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 via a Sophos anti-virus scan before use.

- Only the Computing Subject Lead and Western Business Systems (IT Tech Support) have the administrator rights to install/download software/apps on the school's network, PC's, laptops iPads and Chromebooks. Requests from teachers to download software/apps to enhance their teaching and pupils learning must be made to the Computing subject lead
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
- Unique user authentication logins for all staff and pupils enables Netsweeper monitoring to identify inappropriate internet use/safeguarding issues.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Password Policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year 1, all learners are provided with their own unique username and password to access the school's Chromebooks and their Google Workspace for Education accounts.

We require all users to:

- Use strong passwords for access into our system.
- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

Audit/Monitoring/Reporting/Review*:*

The Headteacher(DSL) will ensure that full records are kept of:

- User Ids and requests for password changes;
- User log-ins;
- Security incidents related to this policy and procedures.
- In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes.
- User lists, IDs and other security related information are stored securely in the school office.

Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- Staff or pupil's personal information will not be published on our website; the contact details on the website will be our school address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.

- The school website will comply with the school’s guidelines for publications including respect for
  intellectual property rights, privacy procedures and copyright.

Managing emails

Staff Emails

All members of staff are provided with a school 365 email address to use for all official school communication. All user school accounts are disabled once the member of the school has left. Prompt action on disabling accounts will prevent unauthorised access.

Staff should ensure:

- The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail.
- Their communications are always professional in tone and content.
- They are aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies..
- Personal email addresses, text messaging, public chat and social networking programmes are not be used for communications with parents/carers and children.
- They change their email passwords every 90 days for security reasons.
- Any electronic communication, which contains sensitive or personal information, will only be sent using secure and encrypted email.
- School email addresses and other official contact details are not used for setting up personal social media accounts.
- Personal email accounts will not be used on school devices
- Staff will not use the school wifi on personal devices.

Pupil Emails

- Pupils normally use only a class email account to communicate with people inside school and with the permission / guidance of their class teacher during a computing lesson
- A structured education program is delivered to pupils, from Year 2 onwards, which helps them to be aware of the dangers of and good practices associated with the use of email
- Pupils are educated on email safety issues, such as the risks attached to the use of personal details.
- They are taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and politely (not include any unsuitable or abusive material)
- Pupils are made aware they must immediately report to their class teacher / Online Safety Coordinator receipt of any email that makes them feel uncomfortable is offensive, threatening or bullying in nature and they must not respond to any such email.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- We gain parental permission for the use of digital photographs or video involving their child as part of the school agreement form when their child joins the school. This is a once in a school lifetime consent.
- Parents are required to inform the school if their consent changes.
- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public their private information.
- Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes. **However**, with the express permission of the Headteacher, images can be taken provided they are transferred **immediately** and solely to the school network, website or Twitter account and then **deleted** from the staff device.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.

  We teach them about the risks associated with providing information with images that reveals the identity themselves or others and their location, such as house number, street name or school.
- We teach them about the need to keep their data secure and what to do if they are subjected to bullying or abuse.

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- If specific pupil photos (not group photos) are published on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long-term use.
- Pupils' full names will not be used anywhere on the school website or Twitter blog, particularly in association with photographs.
- Pupil's work will only be published with the permission of the pupil and parents/carers.
- Parents/carers are strongly advised **not** to publish any images, videos or commentary of other people's children on any social media or publishing platform without prior permission from their parent/carer because there may be unknown risk factors in doing so, no matter how innocent it may be.

Social Media
Expectations

- The school uses an official St Leonard's Twitter account to update parents on news and events.
  The Headteacher is the account manager responsible for approving content and monitoring use of the account.
- Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil Acceptable Use Agreements including clear reporting mechanisms.
- Staff ensure that no reference is made in social media to pupils, parents or other staff and do not engage in online discussions on personal matters about any member 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.
- The school will control access to social media and social networking sites.
- Staff wishing to use Social Media tools with pupils as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Newsgroups i.e. Facebook, Instagram etc. (with the exception of the managed school Twitter account) are blocked in school.
- Concerns regarding a pupil's use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents, particularly when concerning the underage use of sites.
- All members of St Leonard's School community are expected to engage in social media in a positive, safe and responsible manner.

Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our Code of Conduct/Behaviour / Acceptable Use Agreement policies.

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.
    - Civil, legal or 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 sites. 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 the privacy levels of their personal sites.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of St Leonard's School on their personal social networking accounts; this is to prevent information on these sites from being linked with the school, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance 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.

Pupils Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- Any concerns regarding pupils use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Pupils will be advised:
    - To consider the benefits and risks of sharing personal details 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/carers permission and only 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 both within school and externally.

Use of Personal Devices and Mobile Phones

- St Leonard’s School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and ‘smart’ watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - All members of St Leonard’s School community are advised to take steps to protect their mobile phones or 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 St Leonard’s 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 while mobile phones and personal devices should not be shared.
- The sending of abusive or inappropriate messages/content via mobile phones or personal devices, is forbidden by any member of the community; any breaches will be dealt with in accordance with our Code of Conduct / Behaviour policies.

- All members of St Leonard’s School community are advised to ensure that their mobile phones and personal devices do not contain any content that may be offensive, derogatory or would otherwise contravene our behaviour or child protection 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, data security and acceptable use.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place 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 permission has been given by the Headteacher, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy)
- Staff will not use personal devices:
    - To take photos or videos of learners and will only use work-provided equipment for this purpose unless specific permission has been given by the Headteacher (see reference in Use of Digital and Video Images)
    - Directly with pupils and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our Code of Conduct policy
- Staff will not access school wifi on personal devices.
    - 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, the police will be contacted.

Pupils Use of Personal Devices and Mobile Phones

- The school strongly advices that pupil mobile phones should not be brought into school. However, the school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. If this is the case, mobile phones are to be handed to the school office, for safekeeping, at the start and collected at the end of the school day.
- If a pupil needs to contact his/her parents or carers they will be allowed to use the telephone in the school office.
- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in school in accordance with our Acceptable Use Policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) of any breaches our policy.

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, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
  - Pupils, 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 pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, we 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 (or deputy) will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, we will contact the Lancashire Safeguarding Children Partnership or Lancashire Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or deputy will speak with

Lancashire Police and the Safeguarding Children Partnership first to ensure that potential investigations are not compromised.

Concerns about Pupil Welfare

- The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL (or deputy) will record these issues in line with our child protection policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Lancashire Safeguarding Children Partnership procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher, in accordance with the allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however, a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

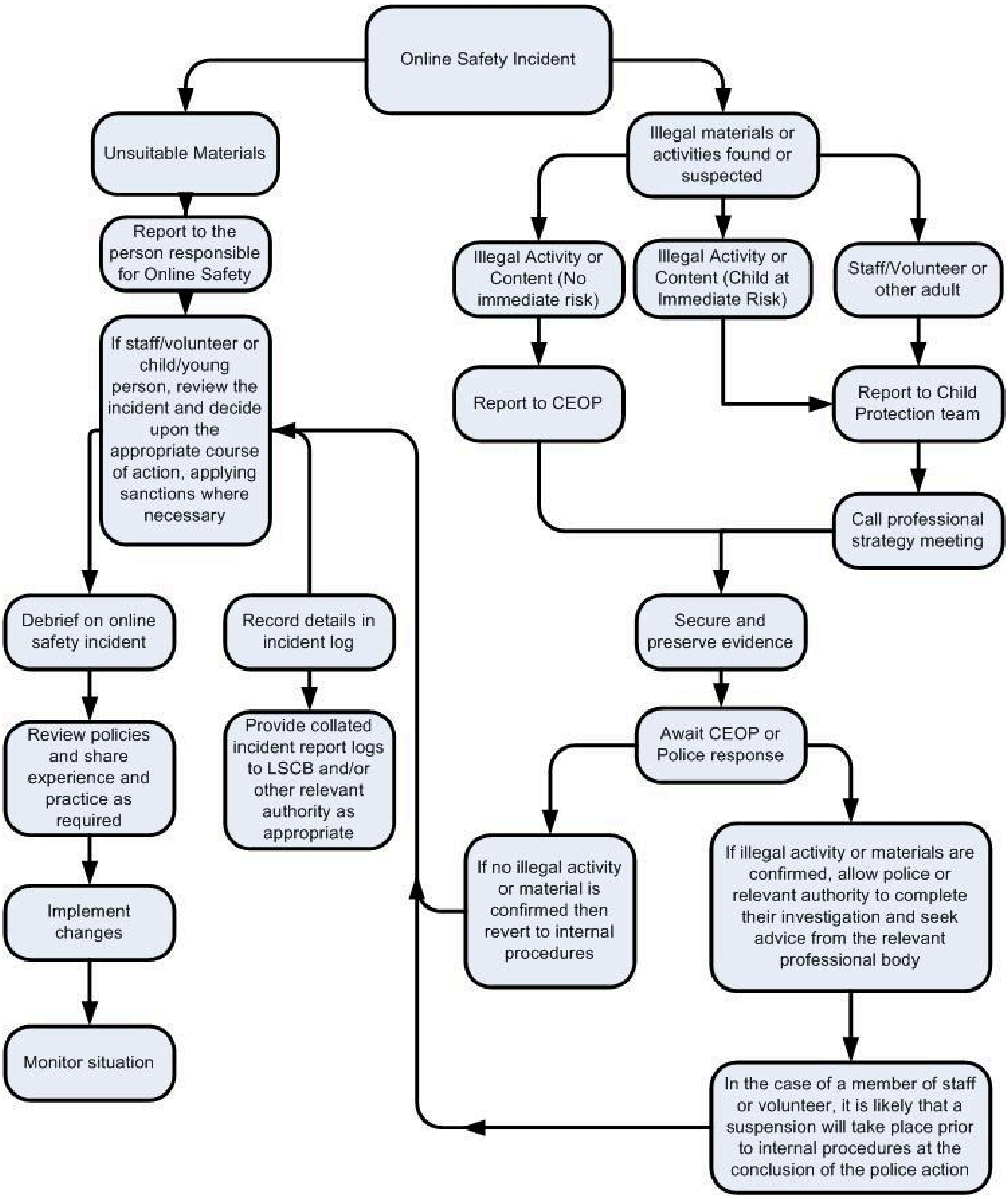
User Actions: Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptabl e	Unacceptabl e and illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
Pornography				X	
Promotion of any kind of discrimination				X	
threatening behaviour, including promotion of physical violence or mental harm				X	
Promotion of extremism or terrorism				X	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X	

Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce				X	
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).
Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible, in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at St Leonard's School .
- Full details of how we will respond to cyberbullying are set out in our Anti-bullying policy.

Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at St Leonard's School and will be responded to in line with existing policies, including 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.

Online Radicalisation and Extremism

- All staff members have received PREVENT training and know how to recognise radicalisation.
- 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 child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the Acting Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Handling a Sexting Incident An overview for all teaching and non-teaching staff in schools and colleges UK Council for Child Internet Safety (UKCCIS)

In the latest advice for schools and colleges (UKCCIS, 2016), sexting is defined as the production and / or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and / or sexual acts. It is also referred to as 'youth produced sexual imagery'. Sexting does not include the sharing of sexual photos and videos of under 18-year olds with or by adults. This is a form of child abuse and must be referred to the police.

What to do if an incident involving sexting comes to your attention:
· Report it to your Designated Safeguarding Lead immediately
· Do not view, download or share the imagery yourself, or ask a child to share or download
· If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL
· Do not delete the imagery or ask the young person to delete it
· Do not ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL
· Do not share information about the incident to other members of staff, the young person(s) it involves or their, or other, parents and/or carers
· Do not say or do anything to blame or shame any young people involved
· Do explain to the child that you need to report it and reassure them that they will receive support and help from the DSL
For further information: Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People (UKCCIS, 2016)