Online Safety Policy (Whole School)

St Christopher's Church of England High School

Approved by:	Governing Body
Last reviewed on:	February 2026
Next review due by:	February 2027

St Christopher's CE High School Mission Statement

St Christopher's is a Church of England Academy where pupils and staff work together, in the knowledge and love of God. We try to act out our faith in daily life, with Christ as our example.

Within our strong Christian, Anglican context, we seek to promote the spiritual, moral, cultural, intellectual and physical development of our pupils, growing together as a caring and supportive community whilst preparing them for the opportunities, responsibilities and experiences of their adult lives.

We aim to achieve our mission by providing an environment which

- recognises that each member of the school community is an individual with specific needs and strengths
- fosters mutual respect and concern for others
- values the contribution made by each member of the school community
- encourages and celebrates positive achievement
- actively supports those in need.

Contents

Introduction

This policy applies to all members of the school community (including staff, pupils, students, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of St Christopher's CE High School, Accrington to safeguard members of our school community online in accordance with statutory guidance and best practice.

St Christopher's will deal with such incidents within this policy, and associated behaviour and anti-bullying policies and will, where known and appropriate, inform parents/carers of incidents of inappropriate online safety behaviour that takes place.

Schedule for development, monitoring & review

This Online Safety Policy was approved by the **school governing body** on:	
The implementation of this Online Safety Policy will be monitored by:	The Senior Leadership Team
The **governing body** will receive updates on the implementation of the Online Safety Policy (which may include anonymous details of online safety incidents) at regular intervals:	As appropriate via the Wellbeing Committee of the Governing Board
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	January 2027
Designated Safeguarding Lead (DSL)	Leanne Williamson
Online Safety Lead (OSL)	Dave Allen
Network Manager	Daniel Pilkington

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents
- filtering and monitoring logs
- internal monitoring data for network activity
- surveys/questionnaires of:
    - pupils
    - parents and carers
    - staff

The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead (DSL), as defined in Keeping Children Safe in Education. Online safety at St Christopher's is further supported by an Online Safety Lead (OSL) and the Network Manager.

Online Safety Policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard pupils and students in the digital world
- describes how the school will help prepare pupils and students to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related Acceptable Use Policies (AUPs)
- is made available to staff at induction and through normal communication channels
- is published on the school website.

Acceptable use

The school has defined what it regards as acceptable/unacceptable use via its Acceptable Use Policies (AUPs).

The AUPs will be communicated/reinforced through:

- staff induction and Code of Conduct
- splash screens
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website.

When using communication technologies, the school considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school. Synergy is the primary form of electronic communication between staff and parents.
- any digital communication between staff and pupils or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to the DSL the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and pupils and students.

Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which may need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing and complaints policies

- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the DSL and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures
- any concern about staff misuse will be reported in line with the school's Child Protection Policy to the Headteacher (or to the DSL, knowing that such will be discussed with the Headteacher), unless the concern involves the Headteacher,(in which case the complaint is referred to the Chair of Governors)
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by pupils and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and fully investigated, the Headteacher will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority
        - police involvement and/or action
- that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents are logged using the school CPOMs recording system (StudentSafe or StaffSafe, as applicable) and may also be recorded under 'Behaviour' on the school's Synergy system.
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as appropriate)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously where appropriate) to:
    - staff, through regular briefings
    - pupils and students, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
    - the Governors' Wellbeing Committee, through safeguarding updates
    - local authority/external agencies, as relevant.

The school will make the flowchart available to staff to support the decision-making process for dealing with online safety incidents.

School actions

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 in-line with the school's Behaviour Policy and Staff Disciplinary and Dismissal Procedure Policy.

The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. Please refer to the school's New and Emerging Technologies Policy which governs the use of AI systems at St Christopher's.

Online Safety Education Programme

Online safety messages will be reinforced across the curriculum including the following:

- Digital competency through the appropriate digital pillars in curriculum areas such as PHSE, ICT and Technology lessons.
- The school incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week to ensure online safety messages are communicated widely.
- The programme will be accessible to pupils and students at different ages and abilities
- Pupils and students will be taught via the curriculum and through assemblies to be critically aware of the materials/ content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)
- Pupils and students will be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services
- Vulnerability is actively addressed e.g., for victims of abuse and SEND.
- Pupils and students will be helped to understand the need for the AUP and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils and students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches Where pupils and students are allowed to freely search the internet, staff should be vigilant in supervising the pupils and students and monitoring the content of the websites / tools (including AI systems) the pupils and students visit
- It is accepted that from time to time, for good educational reasons, pupils and students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Staff / Volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding, data protection and cyber-security training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and AUPs. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- the DSL, OSL and Network Manager will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations

- this Online Safety Policy and its updates will be presented to and discussed by staff at staff meetings/INSET days as appropriate
- advice/guidance/training in relation to online safety will be provided to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of the Wellbeing Committee. This may be offered in several ways such as:

- attendance at training provided by the local authority or other relevant organisations
- participation in school training / information sessions for staff or parents.

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- cyber-security training (at least at a basic level)
- training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and reviews as appropriate.

Families

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers through parents evenings where online safety issues may be discussed
- pupils and students – who are encouraged to pass on to parents the online safety messages they have learned in school
- letters, newsletters and the school website
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications as appropriate and to support parents and carers in managing online safety
- sharing good practice with other schools in clusters as appropriate.

Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering & Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the Network Manager and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours. 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, supported by the OSL for online safety and the Network Manager will have technical responsibility.

Checks on the filtering and monitoring system are carried out by the Network Manager with the involvement of the OSL and DSL. When a safeguarding risk is identified, a review will take place and, where appropriate, there is a change in working practice.

Filtering

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video
The school manages access to content across its systems for all users and on all devices using the schools internet provision including the following:

- the filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the DSL to breaches of the filtering policy, which are then acted upon
- there are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL is involved in the process and aware of the findings. These are shared, as appropriate, with the Wellbeing Committee of the Governing Body
- devices that are provided by the school have school-based filtering applied irrespective of their location
- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/pupils and students, etc.)
- where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

Monitoring

The DfE Technical Standards for Schools and Colleges states:

"Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user's activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything."

The school has monitoring systems in place, agreed by senior leaders and technical staff to protect the school, systems and users:

- The school monitors all network activity across all devices connected to the schools' network.
- The school enforces mandatory user authentication via the web filter to ensure all internet traffic can be matched to specific individuals and devices.
- There are clear protocols for reporting misuse, with a prioritised system for alerts requiring immediate intervention by the DSL.
- All safeguarding alerts are managed in strict accordance with school policy; outcomes are recorded, and all users are informed that monitoring is active.
- Senior leadership, technical staff, the DSL, and the responsible governor conduct a formal yearly review of monitoring provisions to ensure they adapt to new technologies and safety trends.

Technical & Cyber Security

The schools' systems will be managed in ways that ensure that the school meets recommend standards in the DfE technical standards for schools.

- Responsibility for technical security resides with SLT who may delegate activities to identified roles.
- All accounts are governed by the principle of least privilege, ensuring users only have the minimum access required for their specific roles.
- Password policy rules are enforced at domain level to ensure all users utilise a strong password.
- Users are strictly responsible for their own login credentials, must never share account details, and are required to immediately report any suspected security breaches.
- The school utilises Single Sign-On to streamline the login process, providing users with seamless access to multiple services through a single account and reducing the need for multiple sets of credentials.
- System critical administrator passwords are stored in a secure place on encrypted media.
- Network infrastructure and physical systems are securely located with physical access restricted.
- The school has an effective backup and restoration plan in place in the event of cyber attacks; The school adheres to the 3-2-1 backup strategy, maintaining at least three copies of data across two different storage media, with one copy stored securely off-site to ensure robust disaster recovery.
- The IT support team performs daily system checks to monitor functionality and security, aiming to identify and remediate potential issues before they impact users.
- Multi-Factor Authentication (MFA) and geographic location policies are mandatory for all staff accessing school systems off-site, ensuring connections are only permitted from authorised countries.
- The school's disaster recovery procedure is reviewed on an annual basis by the technical team and Senior Leadership Team (SLT) to ensure it remains robust and effective.
- Care will be taken when using AI services inline with the school New and Emerging Technologies Policy.
- All users have been made aware of, and adhere to the school AUPs.
- The school will conduct a cyber risk assessment annually to ensure compliance with the DfE Cyber security standards for schools and colleges. This is reviewed annually by the Network Manager.
- Staff and Governors receive training on the common cyber security threats and incidents that schools experience.
- The school's education programmes include cyber awareness for pupils and students.
- There are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

Social Media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils and student through:

- ensuring that detailed personal information is not published (e.g. by only using first names and, where necessary, an initial) in any posts to the school's social media accounts)
- providing education to help pupils and students to understand the risks, including acceptable use, age restrictions, the risks of digital and video images and data protection
- clear reporting guidance, including responsibilities, procedures, and sanctions
- guidance for parents/carers via parental communications.

School staff should ensure that:

- no reference is made via their personal social media to pupils / students, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of personal information being shared more widely
- they act as positive role models in their use of social media.

Staff should refer to the Code of Conduct for further guidance.

When official school social media accounts are established, there is:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts
- systems for reporting and dealing with abuse and misuse.

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

Digital & Video Images

- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- School should be aware of those pupils and students whose images must not be taken/published and staff should request such information before any images are published.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/ made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils and students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow communicated school procedure concerning the sharing, storage, distribution and publication of those images.
- Care should be taken when sharing digital/video images that pupils and students are appropriately dressed.
- Pupils and students must adhere to the Mobile Phone Policy and Protocol in place in school and must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils and students will be selected carefully.
- Written permission from parents or carers will be obtained before photographs of pupils and students are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes.
- Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school Data Protection Policy.
- Images will be securely stored.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Synergy system
- Public-facing website
- Social media
- Online newsletters.

The school ensures that the Online Safety Policy has been followed in the use of online publishing ensuring that there is least risk to members of the school community, through such publications.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and AUPs; curating latest advice and guidance; providing an online safety page on the school website.

The school Synergy system includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation. The school:

- has a Data Protection Policy
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are within the Data Protection Policy
- has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff
- ensures that where AI services are used, data privacy is prioritised.

When personal data is stored on any mobile device the:

- data will be encrypted, and password protected
- device will be password protected
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices
- 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, a secure email account (where appropriate), and secure password protected devices
- do not use removable media (eg. USB sticks/drives) at any time.

Outcomes

The impact of this Online Safety Policy and practice is regularly evaluated. This may take place through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, pupils, students and parents/carers. Findings reported to the Wellbeing Committee of the Governing body as appropriate.

Appendix 1: Acceptable Use Policy (Staff)

St Christopher's Church of England High School

ICT Acceptable Use Policy

(All Staff, Supply Teachers, Visitors and Guests)

This policy applies **at all times**, in and out of directed working hours, whilst using school resources (including remote and personal connection to the school network) and equipment. The school reserves the right to withdraw access to IT resources from any staff member, visitor, and guest who behaves in an inappropriate manner or in breach of this policy.

Staff, visitors and guests must::

- ☑ Only access websites and other internet activity that is appropriate for use in school. Examples contrary to these are those pertaining to gambling websites, streaming services and retail (unless for the agreed purposes of classroom provision or resourcing). Staff should consult the Senior Network Manager wherever doubt may exist.
- ☑ Be aware that your actions on the internet are monitored and thus confidential information should not be transmitted by this medium.
- ☑ Be careful of what you communicate to others.
- ☑ Treat others, as they would expect to be treated.
- ☑ Respect copyright, trademarks and intellectual property.
- ☑ Use sensible filenames when saving your documents.
- ☑ Report any incidence of cyber-bullying or dangerous and inappropriate behaviour / content to the Designated Safeguarding Lead (DSL).
- ☑ Ensure that artificial intelligence (AI) must only be used appropriately and always in complete conjunction with the New and Emerging Technologies Policy.
- ☑ St. Christopher's staff must ensure to only use the permitted footer format. Guidance for what this should look like and how to do it are on the school SharePoint and help can be sought by emailing ICTSupport@st-christophers.org.
- ☑ St. Christopher's staff must not use any other footer, they must not embellish or adapt the footer in anyway.
- ☑ The primary form of electronic communication from a St. Christopher's staff member to a parent is via Synergy. If staff do contact parents via email they must do so from their St. Christopher's email address, should copy or blind copy their line manager into the communication and must always use professional language, signing off with their title and not their forename. Parents should be addressed in the same manner and Synergy should be consulted for the avoidance of doubt.
- ☑ Staff must be mindful that any form of written communication which is digital and unencrypted, whether via email or Microsoft Teams is the property of St. Christopher's and may also be requested as evidence in a subject access request (SAR).

Staff, visitors, and guests must not:

- ☒ Tell anyone else your password or log on to the network using someone else's password.
- ☒ Send, access or display offensive messages or pictures, or use inappropriate language.
- ☒ Use the school's IT facilities for sending personal e-mails, the completion of subscription forms or the conduct of monetary business.
- ☒ Take photographs or video of staff, pupils or students without prior permission.
- ☒ Publish on the internet (incl. Facebook or any other social media platforms) material such as text, videos or photographs of staff or pupils without prior permission. This includes using your own resources.
- ☒ Use the school's IT facilities to post anonymous messages, or forward chain messages or access chat programs without permission.
- ☒ Use a USB stick or drive at any time.
- ☒ Save or install MP3, video files, games or third-party programs to the school network.
- ☒ Access any inappropriate websites, or view unsuitable images or videos.
- ☒ Access websites that encourage vandalism, crime, terrorism, racism, eating disorders or suicide.
- ☒ Attempt to circumnavigate the proxy and security systems that are in place.
- ☒ Staff members are strongly advised not to communicate directly with pupils and students. In the event that a member of staff must contact a student or pupil it must be from a St. Christopher's email address to the pupil or student's St. Christopher's email address and the head of department should be copied or blind copied in

Please note:

- ☞ User-areas on the school network will be closely monitored and key staff may review your files and communications to maintain system integrity.
- ☞ Websites that are accessed by pupils are recorded and checked regularly to ensure that all pupils, staff and visitors are safe and adhering to the school's Internet policy.
- ☞ If you access an unsuitable website by accident or encounter any material that makes you feel uncomfortable, you should notify key staff.
- ☞ Failure to follow the school's ICT Acceptable Use Policy will result in loss of access and further disciplinary action may be taken, if appropriate. If applicable, external agencies such as the Police may be involved, as certain activities may constitute a criminal offence.

Key Staff:

In addition to the Headteacher:

Mr D. Pilkington - Senior Network Manager

Mr D. Allen - Assistant Headteacher Responsible for New and Emerging Technologies)

Mrs L. Williamson - Designated Safeguarding Lead).

St Christopher's Church of England High School

ICT Acceptable Use Policy

(Main School Pupils Years 7-11)

This policy applies **at all times**, in and out of school hours, whilst using school resources (this includes internet connection while connected to pupils' own devices whilst using St. Christopher's network) and equipment. The school reserves the right to withdraw access to IT resources from any pupil who behaves in an inappropriate manner.

Pupils must:

- ☑ Only access websites and other internet activity that is appropriate for use in school.
- ☑ Be aware that your actions on the internet are monitored and thus confidential information should not be transmitted by this medium.
- ☑ Be careful of what you communicate to others.
- ☑ Treat others, as they would expect to be treated.
- ☑ Respect copyright, trademarks and intellectual property.
- ☑ Use sensible file names when saving your documents.
- ☑ Report any incidence of cyber-bullying to your form teacher or Head of Year.
- ☑ Artificial intelligence (AI) must only be used at the direction of staff and always in complete conjunction with the New and Emerging Technologies Policy.

Pupils must not:

- ☒ Tell anyone else your password or log on to the network using someone else's password.
- ☒ Send, access or display offensive messages or pictures, or use inappropriate language.
- ☒ Use the school's IT facilities for sending personal e-mails, the completion of subscription forms or the conduct of monetary business.
- ☒ Take photographs or video of staff or pupils without prior permission.
- ☒ Publish on the internet (incl. Facebook or any other social media platforms) material such as text, videos or photographs of staff or pupils without prior permission. This includes using your own resources.
- ☒ Use the school's IT facilities to post anonymous messages, or forward chain messages or access chat programs without permission.
- ☒ Access the Internet during lesson time without the teacher's permission.
- ☒ Save or install mp3, video files, games or third party programs to the school network.
- ☒ Access any inappropriate websites, or view unsuitable images or videos.
- ☒ Access websites that encourage vandalism, crime, terrorism, racism, eating disorders or suicide.
- ☒ Attempt to circumnavigate the proxy and security systems that are in place.

Please note:

- ☞ User-areas on the school network will be closely monitored and staff may review your files and communications to maintain system integrity.
- ☞ Websites that are accessed by pupils are recorded and checked regularly to ensure that all pupils are safe and adhering to the school's Internet policy.
- ☞ If you access an unsuitable website by accident or encounter any material that makes you feel uncomfortable, you should notify your teacher.
- ☞ Failure to follow the school's ICT Acceptable Use Policy will result in loss of access and further disciplinary action may be taken, if appropriate. If applicable, external agencies such as the Police may be involved, as certain activities may constitute a criminal offence.

Key Staff:

In addition to your form teacher, class teacher and head of year please be aware of the following people in school:

Mr D. Pilkington - Senior Network Manager

Mr D. Allen - Assistant Headteacher Responsible for New and Emerging Technologies)

Mrs L. Williamson - Designated Safeguarding Lead).

St Christopher's Church of England Sixth Form

ICT Acceptable Use Policy

(Sixth Form Students)

This policy applies **at all times**, in and out of sixth form hours, whilst using sixth form resources (this includes internet connection while connected to students' own devices whilst using St. Christopher's network) and equipment. The sixth form reserves the right to withdraw access to IT resources from any student who behaves in an inappropriate manner.

Students must:

- ☑ Only access websites and other internet activity that is appropriate for use in sixth form. *This also applies outside of lesson time.*
- ☑ Be aware that your actions on the internet are monitored and thus confidential information should not be transmitted by this medium.
- ☑ Be careful of what you communicate to others.
- ☑ Treat others, as they would expect to be treated.
- ☑ Respect copyright, trademarks and intellectual property.
- ☑ Use sensible file names when saving your documents.
- ☑ Report any incidence of cyber-bullying to your form teacher or Head of Year.

Students must not:

- ☒ Tell anyone else your password or log on to the network using someone else's password.
- ☒ Send, access or display offensive messages or pictures, or use inappropriate language.
- ☒ Use the sixth form's IT facilities for sending personal e-mails, the completion of subscription forms or the conduct of monetary business.
- ☒ Use AI to generate work for assignments, essays or coursework to be submitted for assessment or examinations without appropriate accreditation and always in complete conjunction with the New and Emerging Technologies Policy.
- ☒ Take photographs or video of staff or students without prior permission.
- ☒ Publish on the internet (incl. Facebook or any other social media platforms) material such as text, videos or photographs of staff or students without prior permission. This includes using your own resources.
- ☒ Use the sixth form's IT facilities to post anonymous messages, or forward chain messages or access chat programs without permission.
- ☒ Access the Internet during lesson time without the teacher's permission.
- ☒ Save or install mp3, video files, games or third party programs to the school network.
- ☒ Access any inappropriate websites, or view unsuitable images or videos.
- ☒ Access websites that encourage vandalism, crime, terrorism, racism, eating disorders or suicide.
- ☒ Attempt to circumnavigate the proxy and security systems that are in place.

Please note:

- ☞ User-areas on the sixth form network will be closely monitored and staff may review your files and communications to maintain system integrity.
- ☞ Websites that are accessed by pupils are recorded and checked regularly to ensure that all pupils are safe and adhering to the sixth form's Internet policy.
- ☞ If you access an unsuitable website by accident or encounter any material that makes you feel uncomfortable, you should notify your teacher.
- ☞ Failure to follow the sixth form's ICT Acceptable Use Policy will result in loss of access and further disciplinary action may be taken, if appropriate. If applicable, external agencies such as the Police may be involved, as certain activities may constitute a criminal offence.

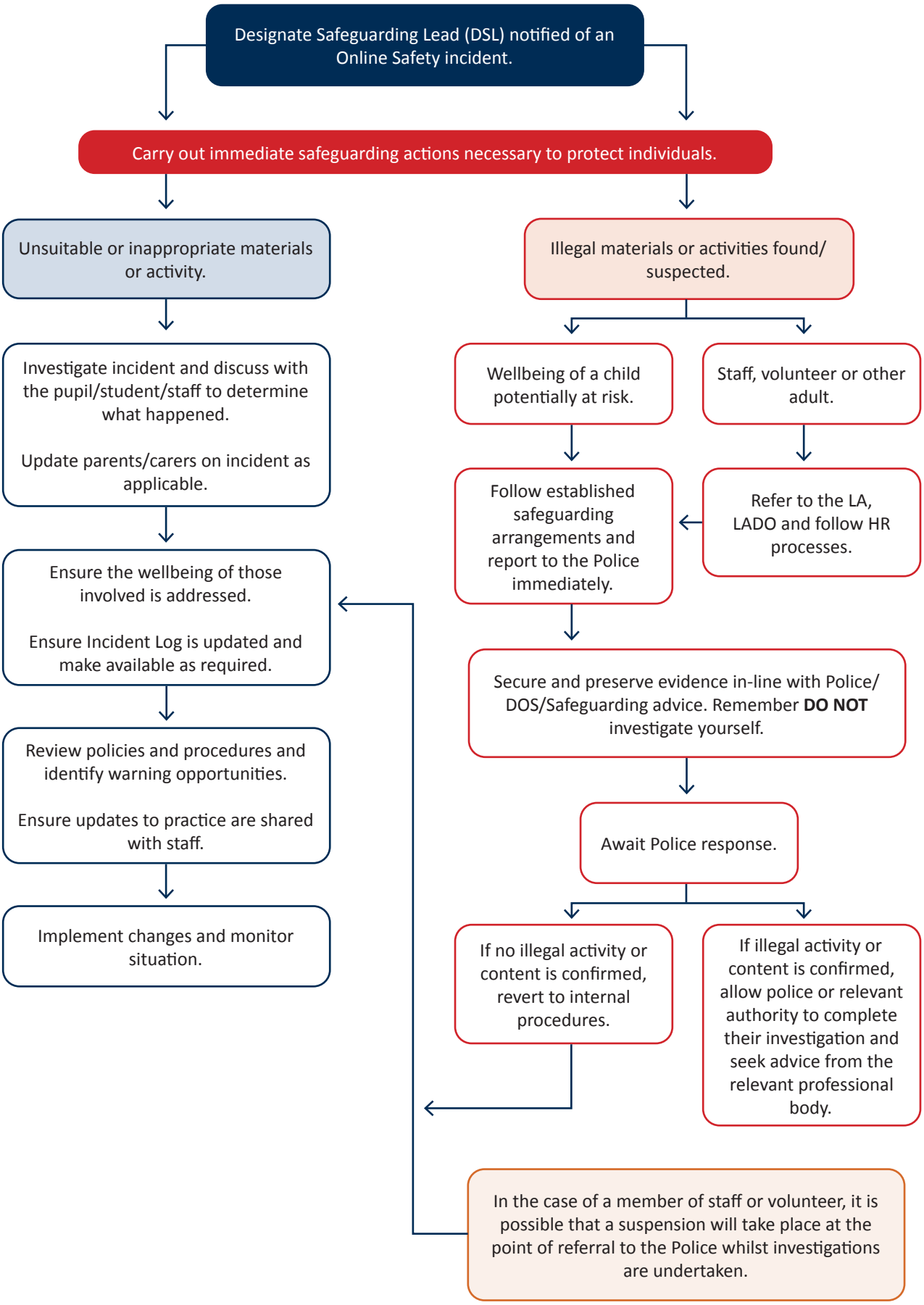
To be completed by the student:

I agree to the school's Acceptable Network and Internet Use Policy and understand that the school reserves the right to examine or delete any files that may be held on its computer systems and monitor the internet sites visited by students.

Full Name: ..... Form: .....

Signature: ..... Date: .....

Appendix 4: Online Safety Incident Flowchart of Actions



That person is like a tree planted by streams of water, which yields its fruit in season and whose leaf does not wither- whatever they do prospers.

Psalm 1:3

St Christopher's CE High School
Queens Road West, Accrington, Lancashire, BB5 4AY

01254 232 992

www.st-christophers.org