Assisi Catholic Trust

Online Safety Policy

Holy Family Catholic Primary School
Our Lady of Lourdes Catholic Primary School
Our Lady of Ransom Catholic Primary School
Sacred Heart Catholic Primary School
St George's Catholic Primary School
St Helen's Catholic Primary School
St Joseph's Catholic Primary School
St Teresa's Catholic Primary School
St Thomas More High School

Mission Statement

Our mission is to inspire the children in our care and that our schools place Christ and the teaching of the Catholic Church at the centre of all we do. We believe that every child has a right to educational excellence, and we will strive together in partnership to ensure this happens.

Motto

'Start doing what is necessary, then do what's possible and suddenly you are doing the impossible.'

Date policy last reviewed: 26th March 2025

Committee Responsible: Audit and Risk Committee

Mr M Stewart — Chair of Audit and Risk Committee — Date: 22/05/2025

Mr F McEvoy — Chair of Trustees — Date: 22/05/2025

Online Safety Policy

Contents

Revision History

Version	Date	Details
Version 1.0	19th December 2024	Draft.
Version 1.1	26th March 2025	Draft.
Version 1.2	28th May 2025	Initial release.

1. Introduction

Assisi Catholic Trust understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the Trust. A number of controls are in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our Trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Online Safety encompasses Internet technologies, communications using computers and other electronic devices such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate all members of the school community about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The responsibility for online safety is not solely delegated to technical staff, or those with a responsibility for digital technology but relates to all members of the school community including governors, staff, students, parents, volunteers, and visitors.

2. Roles and Responsibilities

The responsibility for maintaining safe and secure use of electronic and online technologies lies with everyone. However, specific responsibilities for the implementation of this policy, additional safeguarding measures, monitoring, reporting, and training are given to designated individuals.

2.1 Board of Trustees

At Trust level, the Board of Trustees is responsible for:

- The approval of this Online Safety Policy.
- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring that this policy is implemented.

2.2 Local Governing Committee

At individual school level, the Local Governing Committee is responsible for:

- Ensuring that a member of the Local Governing Committee is designated the role of Child Protection Governor and serves as the link Governor for online safety.
- Ensuring the school's Designated Safeguarding Lead's remit covers online safety.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.

- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually.
- Ensuring that the Strategic Leadership Team and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, manage them effectively, and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges embedded within them.

2.3 Headteacher

The Headteacher has a duty of care to ensure the safety, including online safety, of all members of the school community. The Headteacher is responsible for:

- Ensuring the Designated Safeguarding Lead and all other relevant staff receive suitable training and have enough time and resources to enable them to carry out their responsibilities in relation to online safety.
- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Ensuring staff receive regular, up to date and appropriate online safety training and information that includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Ensuring there is sufficient support and financial provision for the installation and implementation of technologies required to fulfil the needs of online safety.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe.
- Ensuring the school obtains consent for the use of images and related information from parents, or pupils where appropriate.
- Liaising with the Trust IT Manager to review the effectiveness of filtering and monitoring systems.
- Liaising with the Trust IT Manager upon review of this policy.

2.4 Designated Safeguarding Lead

The Designated Safeguarding Lead has overall responsibility for Online Safety and is responsible for:

- Undertaking training to understand the risks associated with online safety.
- Recognising the additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Understanding the purpose of record keeping.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.
- Liaising with the Headteacher and Trust IT Manager upon review of this policy.

2.5 Trust IT Manager

The Trust IT Manager has overall responsibility for this Online Safety Policy and is responsible for:

- Providing support in the development and implementation of this policy and associated school procedures.
- Ensuring schools meet required online safety technical requirements and any relevant online safety guidance that may apply.

- Ensuring that school filtering and monitoring systems are updated as appropriate.
- Overseeing the review of the Trust Online Safety Policy annually and presenting recommendations for adjustment to the Executive Leadership Team.

2.6 Staff

All staff are responsible for ensuring that all members of their school community are safe in all aspects of school life including during the use of electronic and online technologies. Staff are responsible for:

- Having an up-to-date awareness of online safety, the Trust Online Safety policy, and their own school procedures and relevant, related polices.
- Taking responsibility for the security of digital technology and data they use or have access to.
- Modelling good online behaviours and maintaining a professional level of conduct in their personal use of technology.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting any concerns in line with their school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Ensuring they read, understand and adhere to the ICT Usage & Code of Practice for Staff (Appendix B).
- Ensuring students understand and follow the ICT Usage & Code of Practice for Students (Appendix A).

2.7 Students

All students have a responsibility to ensure that they and their fellow students remain safe when using electronic and online technologies. Students are responsible for:

- Adhering to the schools ICT Usage & Code of Practice for Students (Appendix A).
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Understanding the importance of reporting abuse, misuse, or access to inappropriate materials.
- Understanding the importance of adopting good online safety practice when using electronic and online technologies in and outside of the school setting.

2.8 Parents

Parents and carers play a crucial role in ensuring that their children understand the need to use electronic and online technologies in an appropriate way. Schools will take every opportunity to help parents understand these issues through parents' evenings, guest speakers, workshops, newsletters and resources published on the school's website. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow other related guidelines.

3. Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The Designated Safeguarding Lead at each school has overall responsibility for the school's approach to online safety, with support from deputies and the Headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The Designated Safeguarding Lead should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training.
- Staff receive regular updates regarding online safety and any changes to online safety guidance or legislation.
- Online safety is integrated into learning throughout the curriculum.
- Assemblies are conducted on the topic of remaining safe online.

3.1. Handling Online Safety Concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policies.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may still be shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully. The reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

- Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates with relevant staff members and manages concerns in accordance with relevant policies depending on their nature.
- Concerns regarding a staff member are reported to the school's Headteacher.
- Concerns regarding a Headteacher are reported to the school's Local Governing Body, Chair of Governors.
- Concerns regarding a member of the Trust Board are reported to the Chair of Trustees.

Where there is a concern that illegal activity has taken place, the Headteacher contacts the police.

School's will avoid unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with Child Protection and Safeguarding Policies.

All online safety incidents and the school's response are recorded by the DSL.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages.
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras.
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible.
- Threatening or bullying emails possibly sent using a pseudonym or someone else's name.
- Unpleasant messages sent via instant messaging.
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites.
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse.
- Discriminatory bullying online i.e. homophobia, racism, misogyny, misandry.

School's will be aware that certain pupils can be more at risk of abuse and, or, bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur.

5. Child-on-Child Sexual Abuse and Harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence.
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks.
- Sexualised online bullying, e.g. sexual jokes or taunts.
- Unwanted and unsolicited sexual comments and messages.
- Consensual or non-consensual sharing of sexualised imagery.
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse.

All staff will be aware of, and promote, a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

School's will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking 'sides', often leading to repeat harassment.

School's will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with relevant policies and procedures.

6. Grooming and Exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

6.1 Child Sexual Exploitation (CSE)

CSE often involves physical sexual abuse or violence, however, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

6.2 Child Criminal Exploitation (CCE)

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.
Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with Child Protection and Safeguarding Policies.

6.3 Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty.

7. Mental Health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with relevant policies and procedures.

8. Online Hoaxes and Harmful Online Challenges

For the purposes of this policy, an 'online hoax' is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, 'harmful online challenges' refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online. The latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policies.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and Headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

9. Cybercrime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

9.1 Cyber-enabled Crime

Crimes that can be carried out offline but are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.

9.2 Cyber-dependant Crime

Crimes that can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

School's will factor into their approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cybercrime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cybercrime and divert them to a more positive use of their skills and interests.

The DSL and Headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

In addition, school's will implement a cyber awareness plan for pupils and staff to ensure that they understand the basics of cyber security and protecting themselves from cybercrime.

10. Training Staff

Safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

11. Educating Students

Online safety is embedded throughout the curriculum and is always appropriate to pupils' age and developmental stage.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online.
- How to recognise techniques used for persuasion.
- Acceptable and unacceptable online behaviour.
- How to identify online risks.
- How and when to seek support.
- Knowledge and behaviours that are covered in the government's online media literacy strategy.

The online risks pupils may face online are always considered when developing the curriculum.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENDCo and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

School's will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being, or has been, abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the school's Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the school's Child Protection and Safeguarding Policy.

12. Use of Technology in the Classroom

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Internet
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time and this supervision will be suitable to their age and ability.

13. Use of Smart Technology

While the Trust recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which each school will ensure it manages. Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the ICT Usage and Code of Practice for Students (Appendix A) and ICT Usage and Code of Practice for Staff (Appendix B).

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the Internet in a way that breaches the ICT Usage and Code of Practice for Students. Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom.
Where it is deemed necessary, a school will ban pupil's use of personal technology whilst on school site.

School's will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

School's will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

School's will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating Parents

School's will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children.

Parents will be made aware of the ICT Usage and Code of Practice for Students at the beginning of each academic year.

Parents will be made aware of various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents evenings
- Guest speakers and workshops
- Newsletters
- Online resources

15. Filtering and Monitoring

Local Governing Committee's will ensure schools have appropriate filters and monitoring systems in place that meet the DfE's 'Filtering and monitoring standards for schools and colleges'. The Local Governing Committee will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

The Trust IT Manager will ensure annual checks of the filtering and monitoring systems take place to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system(s) will be directed to the Headteacher. Reports of inappropriate websites or materials will be made to the DSL immediately, who will investigate the matter and escalate to the Headteacher and Trust IT Manager to undertake necessary changes as appropriate.

Deliberate breaches of the filtering system will be reported to the DSL, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the school's behaviour policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the school's staff code of conduct and disciplinary procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and, or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the school's Child Protection and Safeguarding Policy.

Technical security features, such as anti-virus software, will be kept up-to-date and managed by the Trust IT Manager and appropriate IT Support personnel. Firewalls will be enabled at all times.

Filtering and Monitoring systems will be implemented and maintained in line with the Trust Filtering and Monitoring Policy (Appendix H).

16. Email

Access to, and the use of emails, will be managed in line with the ICT Usage and Code of Practice agreements. Information will be provided on how to spot fake emails and phishing scams using the Spotting Fake Emails and Protecting Yourself Guidance (Appendix E).

Any cyber-attacks initiated through emails will be managed in line with the Trust Cyber Response Plan.

17. Artificial Intelligence (AI)

School's will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' ages.

School's will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

School's will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

18. Mobile Phones and Social Media

The use of mobile phones and social media by staff and pupils will be managed in line with Use of Mobile Phones and Social Media Policy (Appendix G).

19. Monitoring and Review

This plan will be reviewed, and the results recorded, according to the following schedule:

- Annually.
- Subsequent to a change in IT infrastructure or process.
- Subsequent to any online safety incidents.

20. Appendices

Appendix A: ICT Usage and Code of Practice for Students
Appendix B: ICT Usage and Code of Practice for Staff
Appendix C: Privileged User Accounts Policy
Appendix D: ICT Usage and Code of Practice for IT Administrators
Appendix E: CCTV Code of Practice and Usage Policy
Appendix F: Safe Use of Images Guidance Policy
Appendix G: Use of Mobile Phones and Social Media Guidance Policy
Appendix H: Filtering and Monitoring Policy
Appendix I: Email Approval Process Flowchart

Appendix A

Assisi Catholic Trust

ICT Usage & Code of Practice for Students

Introduction

The ICT System is owned by the school and may be used by students to further their education. The ICT Usage & Code of Practice for Students has been drawn up to protect all parties including students, staff, parents, guardians, and the school. The school reserves the right to monitor all Internet access including access made via personal devices when connected to the school network. The school reserves the right to monitor internet access and examine or delete any files that may be accessed or held on its ICT System.

All students must agree to this ICT Usage & Code of Practice.

1. Acceptable use of the ICT System

The following constitutes acceptable use of the school's ICT System by an individual.

1.1 Students must keep all account passwords secure.
1.2 Students must refrain from deleting system files, applications, or other students' work, or modify system or workstation settings.
1.3 Students must refrain from attempting to gain access to unauthorised areas of the network or another user's documents area.
1.4 Students must not knowingly transfer malicious software to the network.
1.5 Students must not attempt to damage the ICT systems, including hardware and software.
1.6 Students must not attempt to install any software, applications, or device drivers onto any school computer.

2. Acceptable use of the Internet, email, and virtual learning platforms (VLP)

All Internet activity should be appropriate to the student's education. The following constitutes acceptable use of the Internet, email and all school provided access to virtual learning platforms by an individual.

2.1 Students must respect copyright of material.
2.2 Students must not undertake any Internet activity not appropriate to the school's aims and Catholic ethos.
2.3 Students must not undertake activity that threatens the integrity of the school ICT system or that may attack or corrupt other systems.
2.4 Students must not undertake activities for personal financial gain, gambling, political purposes, or advertising.
2.5 Students must not undertake activities that access inappropriate materials, such as pornographic, racist, or offensive material.
2.6 Students must report inadvertent access to inappropriate websites immediately to their teacher or available member of staff.
2.7 Students must access email and any VLP only via an authorised account and password.
2.8 Students must apply the same high standard of language and content to email as you would for letters or other public communication.
2.9 Students must not attempt to bypass the schools Internet filtering by means of alternative or unauthorised software including Internet browsers or web based anonymous proxies.
2.10 Students must refrain from downloading games or executable files not associated to their learning.
2.11 Students accept that all Internet access made using a school provided device, including that which is encrypted, is subject to inspection by the school's web filtering systems.

3. Acceptable use of social media networking sites

The following constitutes acceptable use of social media networking sites by students.

3.1 Students must not access personal social media networking accounts using a school provided device.
3.2 Students must not use their personal equipment to access social media networking sites in school.
3.3 Only students with school authorisation to access specific social media networking sites may do so.
3.4 Inappropriate use of social networking sites that brings the schools catholic ethos and good name into disrepute, either within the school, or privately, could lead to disciplinary action.

4. Acceptable use of the wireless network

The following constitutes acceptable use of the school's wireless network by an individual using a personal device.

4.1 Where appropriate to the location, students must only connect personal wireless enabled devices to the designated student wireless network.
4.2 Students must not attempt to gain access to any other school wireless network.
4.3 Students must not attempt to gain access to a school wireless network using any account other than their own.
4.4 Students accept that all Internet access made using a personal device, including that which is encrypted, is subject to inspection by the school's web filtering and threat management systems.

5. Acceptable use of a school provided laptop

Laptops are provided to students to support their learning. No other person is authorised to use a school provided laptop including parents, guardians, family, or friends for activities that do not support the students learning. Students must return a school provided laptop to the school upon request.

6. Maintenance of a school provided laptop

Maintenance tasks will be undertaken by designated members of staff. This includes system updates and upgrades to software applications to ensure the school complies with licensing agreements.

6.1 Students must not remove, reinstall, modify, or upgrade the operating system.
6.2 Students must not partition or format the laptop storage drive.
6.3 Students must report any error messages to the class teacher.

7. Security of a school provided laptop

Students are advised to make every reasonable attempt to keep the laptop safe and avoid damage.

7.1 Students must lock the laptop away, out of sight when it is left unattended, both in and out of school.
7.2 Students must use the laptop in the UK only. Should a pupil wish to use a laptop outside of the UK, permission must be sought from the Headteacher.

8. Insurance covering a school provided laptop

The school's insurance policy covers theft or attempted theft by forcible or violent means whilst the laptop is at the students' place of residence. The school's insurance policy states that insurers will not be liable for theft or attempted theft from a car unless the laptop is stored out of sight in a locked boot, with all doors, windows, and other openings securely locked and properly fastened and entry to the vehicle has been gained by forcible and violent means.

9. General care of a school provided laptop

The following guidelines are given to help ensure a laptop provides several years of service.

9.1 Students should not leave the laptop in extremes of temperature.
9.2 Students should not clean the laptop with chemicals or abrasive cloths/brushes.
9.3 Students should not consume food or drink around the laptop.
9.4 Students should store the laptop in a cool, dry environment in a safe and secure place.
9.5 Students should ensure there is nothing on the keyboard when the lid of the laptop is closed.

10. Revision History

Version 1.0	9th January 2014	Draft
Version 1.1	19th March 2014	Initial Version
Version 1.2	12th July 2013	Policy Update
Version 1.3	18th March 2016	Policy Review
Version 1.4	22nd May 2018	Policy Review Addition of revision history (10).
Version 1.5	26th June 2020	Policy Review Addition of parents and guardians to introduction (1). Virtual Learning Environment changed to Virtual Learning Platforms (2). Reference to who can use a school provided laptop added (5). Headings changed to reference provided laptops (5, 6, 7, 8, and 9).
Version 1.6	6th September 2021	Policy Review. No Changes.
Version 1.7	27th October 2022	Policy Review. Minor grammatical changes.
Version 1.8	8th September 2023	Policy Review. No Changes.
Version 1.9	24th September 2024	Policy Review. Section 1.5 updated to elaborate on what is included in 'ICT Systems'. Section 2.10 updated to elaborate on 'downloading games'. Section 6 references to ICT Technical Team updated to IT Support Team. Section 6.2 updated terminology to 'Storage drive'. Section 7.2 updated to permission from Headteacher.
Version 2.0	25th March 2025	Policy Integration with centralised Online Safety Policy. Section 4.1 added 'appropriate locations' for student wireless network access. Section 5 updated to clarify use of a student laptop by a parent or guardian. Section 6.3 updated to reference 'class teacher'.

Appendix B

Assisi Catholic Trust

ICT Usage & Code of Practice for Staff

Introduction

This usage and code of practice policy aims to advise staff on the most effective way to use the school's ICT System in an efficient and safe manner. This guidance aims to protect all parties including the pupils, staff, and the school. By its very nature, the document does give advice on activities that individuals should avoid but this is not intended to restrict lawful and ethical activity. The use of the ICT System must conform to relevant legislation including the General Data Protection Regulation, Copyright, Designs and Patents Acts and the CCTV Code of Practice. The use of the school ICT equipment must be conducted in accordance with the Catholic ethos of the school.

The ICT System, including laptops, are the property of the school and should be used by staff to enhance their professional activities including teaching, research, administration, and management. Staff may use the ICT equipment for both professional and personal purposes, provided it is in accordance with the school's ethos.

All staff must agree to this ICT Usage & Code of Practice.

1. **General Data Protection Regulation**
   All schools in the Assisi Catholic Trust will comply with the six principles contained in the General Data Protection Regulation, any associated legislation, and any future changes of legislation. The principles are:
   - Personal data shall be processed lawfully, fairly, and transparently.
   - Personal data shall be collected only for the specific legitimate purposes.
   - Personal data shall be adequate, relevant, and limited to what is necessary.
   - Personal data shall be accurate and kept up to date.
   - Personal data shall be stored only as long as is necessary.
   - Personal data shall be stored with appropriate security, integrity, and confidentiality.

2. **Digital Data Security**
   To conform with the seventh principle of the General Data Protection Regulation the following constitutes acceptable storage of sensitive or personal data by an individual.

   2.1 Staff must not remove, transfer, upload or copy sensitive or personal data from the school network to any unencrypted removable storage device.
   2.2 Staff must not use any email account other than that provided by the school to remove, transfer, upload, copy or send sensitive or personal data from the school network via email.
   2.3 Staff must ensure that any personal digital device that has access to a work provided email account must be kept secure at all times and secured with a password or PIN code when not in use.
   2.4 Staff must not remove, transfer, upload or copy sensitive or personal data from the school network, or organisation provided cloud-based storage platforms, to Internet based websites including social media sites.
   2.5 Staff must not store images or video of pupils on any personal digital device including digital cameras, mobile phones, or tablets.
   2.6 Staff must not remove, transfer, upload or copy sensitive or personal data from the school network to any personal cloud-based storage platform.

3. Acceptable use of the ICT System

The following constitutes acceptable use of the school's ICT System by an individual.

3.1 Staff must agree that the school may examine or delete any files that are held on its ICT System.
3.2 Staff must agree that the school may monitor Internet activity, and any emails sent and received.
3.3 Staff must report any inappropriate material found on the school network or misuse of the school's ICT systems by either staff or pupils to the Headteacher or his/her deputy.
3.4 Staff must log off or lock workstations left unattended to ensure the integrity and security of data held.
3.5 Staff must keep all account passwords secure.
3.6 Staff must refrain from deleting system files, applications or other staff or pupils' work, or modify system or workstation settings.
3.7 Staff must refrain from attempting to gain access to unauthorised areas of the network or another user's documents.
3.8 Staff must not knowingly transfer malicious software to the network.
3.9 Staff must refrain from downloading games or executable files. IT Support staff will assist staff who require subject specific executable files as part of their professional activity.
3.10 Staff must not attempt to damage the ICT systems, as this will be treated as a disciplinary offence.
3.11 Staff must not allow pupils to access the computer network using a staff username and password.
3.12 Staff must delete sensitive or personal data when it is no longer required.

4. Acceptable use of the Internet, email, and Virtual Learning Platforms (VLP)

Due to continuing advances in technology, it is not possible to guarantee safety when using the Internet. However, by working within the guidance given below, the risks can be reduced, and the school and its staff and pupils can be protected.

The following constitutes acceptable use of the Internet, email, and virtual learning platforms by an individual.

4.1 Staff must respect copyright of material.
4.2 Staff must not undertake any Internet activity not appropriate to the school's aims and Catholic ethos.
4.3 Staff must not undertake activity that threatens the integrity of the school ICT System or that may attack or corrupt other systems.
4.4 Staff must not undertake activities for personal financial gain, gambling, political purposes, or advertising.
4.5 Staff must not undertake activities that access inappropriate materials, such as pornographic, racist, or offensive material.
4.6 Staff must report inadvertent access to inappropriate websites immediately to the Headteacher or his/her deputy.
4.7 Staff must access email and any VLP only via an authorised account and password.
4.8 Staff must apply the same high standard of language and content to email as you would for letters or other public communication.
4.9 Staff are responsible for any email sent or content published on a VLP or any other public website.
4.10 Staff must not post anonymous messages or forward chain letters.
4.11 Staff must use a school email address for all school related electronic communication. Personal email must be sent, and received, using a separate, private email account.
4.12 Staff must not use peer-to-peer file sharing software. This is strictly prohibited.

5. Acceptable use of social media networking sites

The following constitutes acceptable use of social media networking sites by staff.

5.1 Staff must not use their personal equipment to access social media networking sites in the school whilst in the vicinity of students when in public areas including classrooms, corridors other public areas and whilst on duty.
5.2 Staff may use their personal equipment to access social media networking sites in the school away from the vicinity of students when in private areas including the staff room and offices.
5.3 Only staff with school authorisation to access specific social media networking sites may do so.
5.4 Inappropriate use of social networking sites that brings the schools catholic ethos and good name into disrepute, either within the school, or privately, could lead to disciplinary action.
5.5 It is prohibited to 'friend' any student on roll on any social media networking sites unless authorised by the school.

6. Acceptable use of the wireless network

The following constitutes acceptable use of the school's wireless network by an individual using a personal device.

6.1 Where appropriate to the location, staff must only connect personal wireless enabled devices to the designated staff wireless network.
6.2 Staff must not attempt to gain access to any other school wireless network.
6.3 Staff must not attempt to gain access to a school wireless network using any account other than their own.
6.4 Staff accept that all Internet access made using a personal device, including that which is encrypted, is subject to inspection by the school's web filtering and threat management systems.

7. Acceptable use of a school laptop

Laptops are for the use of staff to support their professional and personal activities. Staff must not allow anyone else to use a work laptop. Use by students, family or friends is prohibited. Staff must return a school provided laptop to the school upon request.

7.1 Staff must have the laptop available for use in school every day.
7.2 Staff must save work created for school use in the 'Documents' area of the laptop. Personal files must be stored on the local storage drive and are not backed up to the cloud. The member of staff takes full responsibility for making backup files of any personal data.
7.3 Staff must log off from the network when the laptop is not in use.
7.4 Staff must not install unapproved or unlicensed software onto the laptop.
7.5 Staff must return the laptop to the school upon request.
7.6 Staff must ensure that in the event of leaving employment at the school, the laptop is returned to the school prior to the last working day.

8. Maintenance of a school laptop

Maintenance tasks will be undertaken by IT Support staff. This includes system updates and upgrades to software applications to ensure the school complies with licensing agreements.

8.1 Staff must not remove, reinstall, modify, or upgrade the operating system.
8.2 Staff must not partition or format the laptop storage drive.
8.3 Staff must not remove, reinstall, modify, or upgrade any software that is installed when the laptop is first issued.

9. Damage to, or loss of, a school laptop

Staff are responsible for their equipment at all times whether on the school premises or not.

9.1 Staff must keep equipment in good condition.
9.2 Staff must report any equipment damage immediately.
9.3 Staff may be held responsible for replacement costs if damage, or loss, is deemed to have occurred through negligence or malice.

10. Security of a school laptop

Staff are advised to make every reasonable attempt to keep the laptop safe and avoid damage.

10.1 Staff must not remove, modify, upgrade, or disable the antivirus software.
10.2 Staff must not install any additional antivirus or firewall software.
10.3 Staff must not remove, modify, upgrade, or disable the encryption software.
10.4 Staff must not remove, modify, or alter any encryption configuration settings.
10.5 Staff must lock the laptop away, out of sight when it is left unattended, both in and out of school.
10.6 Staff must use the laptop in the UK only. Should a member of staff wish to use a laptop outside of the UK, permission must be sought from the Headteacher or designated responsible person.

11. Insurance covering a school laptop

The school's insurance policy covers theft/attempted theft by forcible or violent means whilst the laptop is at the staff member's place of residence. The school's insurance policy states that insurers will not be liable for theft/attempted theft from a car unless the laptop is stored out of sight in a locked boot, with all doors, windows,

and other openings securely locked and properly fastened and entry to the vehicle has been gained by forcible and violent means.

12. General care of a school laptop

The following guidelines are given to help ensure a laptop provides several years of service.

12.1 Staff should not leave the laptop in extremes of temperature.
12.2 Staff should not clean the laptop with chemicals or abrasive cloths/brushes.
12.3 Staff should avoid consuming food or drink around the laptop.
12.4 Staff should store the laptop in a cool, dry environment in a safe and secure place.
12.5 Staff should ensure there is nothing on the keyboard when the lid of the laptop is closed.

11. Revision History

Version 1.0	20th January 2013	Draft
Version 1.1	29th January 2013	Initial Version
Version 1.2.1	12th July 2013	Policy Update
Version 1.2.2	19th May 2015	Policy Review
Version 1.3	18th March 2016	Policy Review
Version 1.4	22nd May 2018	Policy Review Revision of Data Protection Guidance in line with new legislation (1). Update to digital data security to reference GDPR (2). Addition of revision history (12).
Version 1.5	23rd October 2019	Policy Review
Version 1.6	26th June 2020	Virtual Learning Environment changed to Virtual Learning Platforms (2). Addition of request to return laptop to school added (7). Headings standardised (7, 8, 9, 10 and 11).
Version 1.7	6th September 2021	Policy Review. No Changes.
Version 1.8	27th October 2022	Policy Review. No Changes.
Version 1.9	8th September 2023	Policy Review. No Changes.
Version 1.10	24th September 2024	Policy Review. Section 7 and 8 references to ICT Technical Team updated to IT Support Team. Section 7.2 terminology updated to 'Storage drive' and 'the Cloud'. Section 7.3 removed. No longer relevant. Section 8.2 terminology updated to 'Storage drive'.
Version 2.0	25th March 2025	Policy Integration with centralised Online Safety Policy. Section 1 updated to reference all schools in the Assisi Catholic Trust. Section 2.4 updated to reference cloud-based storage platforms. Section 2.5 updated to reference tablets. Section 3.7 removal of 'area' terminology. Section 3.9 updated to reference IT Support staff. Section 6.1 added 'appropriate locations' for student wireless network access. Section 7.4 updated to remove reference to software licences. Section 8 removal of references to the IT Support Team. Section 9 added. Section 10.6 updated to reference Headteacher. Section 12 updated to align with current technologies.

Appendix C

Assisi Catholic Trust

Privileged User Accounts Policy

Introduction

Network and systems administrators have privileges and duties that may bring them into contact with sensitive, restricted, or personal information during the course of their work. The purpose of this document is to ensure that administration roles and responsibilities are properly understood and that privileged accounts are used appropriately.

These guidelines apply to all personnel, including those providing services under contract, who are provided with Administrator or Privileged Access to school computing and information resources. This includes hardware systems and software applications.

1. **Definitions**
   Anyone with access that enables them to affect change that would be felt beyond their immediate job role could be considered a privileged user. For example, administering systems or networks which are critical to a business (e.g., database admins) or accessing systems used to perform a critical function (e.g., approving financial payments). Privileged Access is therefore defined as a level of access above that of a 'normal' user.

2. **Examples of users with privileged access:**
   - A School Business Manager account with the ability to process payments.
   - An external IT Support Technician account providing access to a server.
   - A DSL account with read/write access to a safeguarding reporting application.
   - A curriculum subject leader account with access to add/remove users from a curriculum app.

3. **Types of Administrative Accounts**

   - **Local Administrative Accounts**
     Non-personal accounts that provide administrative access to the local host or instance only.
     Example: Staff member who has been given an admin account to make changes, add users, or perform maintenance on a specific workstation or laptop.

   - **Application Administrative Accounts**
     Accounts used by applications to access databases, external third-party applications, or services.
     These privileged accounts usually have broad access to underlying company information that resides in applications and databases.
     Example: Administration staff with write access to the schools Management Information System (MIS).

   - **Domain Administrative Accounts**
     Privileged administrative access across all workstations and servers in one, or more than one, domain.
     These accounts provide the most extensive access and any compromise to the security of this type of account is serious and puts the school at risk.
     Example: IT personnel that monitor connectivity and implement group policy across the whole network.

   - **Emergency Accounts**
     Unprivileged users with administrative access to secure systems in the case of an emergency and are

sometimes referred to as 'break glass' accounts. It is recommended that there are at least two users with privileged access for any system. This reduces the need to make sudden decisions in an emergency. Example: Staff illness prevents admin access, and the school can't provision new accounts or make system modifications. A new admin account is needed to maintain functionality and core business functions.

4. **Privileged User Accounts**

Privileged user accounts have specific additional access to one or more systems or applications.

- Accounts must have unique and complex passwords.
- Monitoring of account use should be undertaken, and access should be periodically reviewed.
- Documentation should be undertaken when staff are granted enhanced access to systems.

User accounts should always follow the 'least privilege' principle. Users should only be provided with accounts with sufficient access for the requirements of their role.

Staff should have separate user accounts if they are expected to perform both administrative and routine functions.

Administrators should log in with standard user accounts for day-to-day tasks.

Privileged user accounts must be approved by the Headteacher (or their deputy) or Chief Financial Officer (or their deputy) in liaison with the Trust IT Manager (or their deputy).

5. **Data Integrity**

Administrators must ensure their activities do not result in the loss or destruction of information.
If a change is made to stored data, then the affected user(s) must be informed of the change and the reason for it as soon as possible after the event.

6. **Monitoring**

Administrators must not act to monitor or enforce policy unless they are sure that all reasonable efforts have been made to inform users that both such monitoring will be carried out, and the policies to which it will apply.

If this has not been done through a general notice to all users (such as the ICT Usage & Code of Practice for staff) then individual permission must be obtained from file owner(s) before a file is examined. If a network communication is monitored, all parties should provide consent before monitoring takes place.

7. **Appropriate Use of Administrator Access**

Privileges provided to administrators are solely for the purposes of supporting the smooth running of the school and to enable the school to ensure maximum availability, data integrity and security for the systems they are responsible for.

The use of Administrator Access should be consistent with an individual's role or job responsibilities as prescribed and authorised by the Strategic Leadership Team. When an individual's role or job responsibilities change, Administrator Access must be reviewed and appropriately updated or removed.

In situations where it is unclear whether a particular action is appropriate, and within the scope of current job responsibilities, the situation should be discussed with the Headteacher or Chief Financial Officer.

8. **Reporting Requirements**

Report any suspected violation of the Trust Online Safety Policy to the Headteacher or Chief Financial Officer. This includes suspected inappropriate use of Administrator Access.

Report any data or security breach concerns to the Headteacher or Trust IT Manager promptly, providing information as to the date, time, location, and potential extent of any breach.

9. **Exceptions**

Requests for exceptions to any information security policies may be granted for documented and explicit reasons with compensating controls in place to mitigate risk.

10. Privileged access review

The following will trigger an automatic review of access and consideration for revocation:

- Notice to leave a post.
- A change of role.
- Contractual expiry.
- Breach of policy or user actions which may lead to disciplinary action.

11. Appendices

Appendix D: ICT Usage and Code of Practice for IT Administrators

12. Revision History

Version 1.0	11th November 2021	Draft
Version 1.1	16th December 2021	Initial Release
Version 1.2	27th October 2022	Policy Review. No Changes.
Version 1.3	8th September 2023	Policy Review. No Changes.
Version 1.4	24th September 2024	Policy Review. Policy rebranded to the Assisi Catholic Trust. Logo and organisation name changed to cover all schools in the Trust. References to IT Manager and Director of Finance and Operations updated to Trust IT Manager and Chief Financial Officer.
Version 2.0	25th March 2025	Policy Integration with centralised Online Safety Policy.

Appendix D

ICT Usage and Code of Practice for IT Administrators

System administrators must:

1. Restrict the use of accounts with privileged access to functions consistent with the administrator's role, job responsibilities, and the purpose for which the access was granted.
2. Ensure that networks, systems, and services are available to authorised users only.
3. Ensure information is handled and transferred correctly, preserving its integrity, and providing an appropriate level of security for the classification of the data being processed.
4. Ensure that default passwords are changed using strong password methodologies when an Information System is installed or implemented.
5. Where necessary, monitor compliance with IT policies which apply to the systems being administrated and act in support of school policies at all times.
6. Monitor and record network traffic if defined as being in the scope of the role.
7. Take steps to ensure adherence to, and compliance with, all hardware and software license agreements entered into and communicated by the school.
8. Examine relevant files as part of necessary security investigation if defined as being in the scope of the role.

In addition to activities deemed inappropriate in the school's ICT Usage & Code of Practice for Staff, IT Administrator's must not:

1. Bypass user access controls or any other formal security controls, without approval.
2. Bypass formal account activation, suspension or change procedures, including enhancing user permissions without authorisation.
3. Bypass security measures or access restrictions applied to protect information or access to information that is outside the scope of specific job responsibilities.
4. Disclose information, accessed as part of authorised works, to those unauthorised to view it.
5. Use additional access to satisfy personal curiosity about an individual, system or school practice.
6. Monitor user activity which is not authorised and/or does not form part of routine monitoring encompassed by school policy.
7. Use administrative accounts when there is not a business need to do so.
8. Attempt to make readable the content of a file or communication that appears to have been deliberately protected by the owner, for example by encrypting it, without specific authorisation from management or the owner of the file.
9. Use administrative credentials to access systems with untrusted devices.

I have read the guidelines for Privileged IT Accounts and agree to abide by the ICT Usage & Code of Practice for IT Administrators.

Name: _____ **Job Role:** _____

Signature: _____ **Date:** _____

Authorised by: _____ **Job Role:** _____

Authoriser Signature: _____ **Date:** _____

Appendix E

Assisi Catholic Trust

Spotting Fake Emails and Protecting Yourself

phishing
noun
1. the practice of using fraudulent emails and copies of legitimate websites to extract financial data from computer users for purposes of identity theft.

There are numerous ways to detect fake sites, emails and phishing scams. Here are 8 tips to protect yourself.

Tip 1: Don't trust the display name
Display names are not secured. This means that anyone in the world can pretend to be sending an email from a legitimate company or person when in fact the origin could be somewhere entirely different. Spoofing the display name of an email is a favourite phishing tactic among cybercriminals. Always check the senders email address.

Tip 2: Look but don't click
Hover your mouse over any links embedded in the body of the email. If the link address looks weird, don't click on it. E.g.: an email claiming to be from Barclays Bank would not have a link pointing to 'www.somebank123.com'.

Tip 3: Don't click on or open attachments
Including malicious attachments that contain viruses, and malware is a common phishing tactic. Don't open any email attachments you aren't expecting or that are from unknown senders.

Tip 4: Vague and blank emails
Often, phishing emails will be sent with very vague or even no written content. These sorts of emails often include attachments. If you feel curiosity towards opening an attachment from an unknown sender, see tip 3 above!

Tip 5: Scrutinise the salutation and spelling
Brands are pretty serious about email. If the email is addressed to "Valued Customer" or "Dear Facebook User" it could be a phishing scam. Legitimate businesses will often use a personal salutation with your first and last name. Legitimate messages usually do not have spelling mistakes or poor grammar. If it looks suspicious ignore it.

Tip 6: Don't give up personal information
Legitimate banks and other companies will never ask for personal credentials, passwords, login details or PIN numbers via email. Don't give them up!

Tip 7: Beware of urgent or alarmist language in the subject line
Invoking a sense of urgency or fear is a common phishing tactic. Beware of subject lines that claim your "account has been suspended!" or your account had an "unauthorized login attempt!"

Tip 8: Don't believe everything you see
Just because an email has convincing logos, language, and a seemingly valid email address, does not mean that it's legitimate. Be sceptical when it comes to your emails and if it looks even remotely suspicious, don't open it.

Appendix F

Safe Use of Images Policy

Generally, photographs and videos for school and family use should be a source of innocent pleasure and pride, which can enhance self-esteem for children and young people and their families. Regrettably, there are occasions when this is not the case and technology such as digital and mobile phone cameras have made the potential for misuse of images easier. The following guidance is intended to apply to all forms of images, whether in print, on film or video, digital, on websites and in the professional media.

1. Introduction

1.1 Photographs and videos can be effective ways to show parents and the local community the activities and learning that take place at our school.

1.2 Using new technologies such as digital cameras and websites makes it easier to take images and show them to the world, but we have a responsibility to make sure that individual and parental rights are respected, and that vulnerable individuals are protected from risk.

1.3 Issues of child protection, data protection and parental consent need careful thought. Images can be used by those who intend harm to children, for example as a preliminary to "grooming" or by displaying them inappropriately on the internet. The risk for an individual child is slight. However, for children that are abused in this way the consequences can be profound.

1.4 It is important to make a balanced judgement on the use of images. Schools are as likely to be criticised for over-reacting as they are for having failed to exercise caution.

2. Getting consent for the use of images of children and young people

2.1 The taking of photographs and videos of children purely for personal use such as by parents at Sports Day or by grandparent's videoing a play is not a breach of the General Data Protection Regulation and is not forbidden by the school.

2.2 Photographs taken for official use may be subject to the provisions of the General Data Protection Regulation. Permission from the person with parental responsibility for a child will therefore be sought before we take their photograph for a publication, website or display in a public place. A public place includes areas where visitors to our school have access.

2.3 The school will get consent to last for the whole period that the child is at school and the year after they have left, to enable us to publicise activities undertaken by final year students. (This is not intended to refer to photographs/videos around the school for the interest of the students. Many of these will show the 'history' of the school, e.g., school plays, sporting achievements etc.).

2.4 The school will send a consent form with the school's registration pack. Yearly reminders will be sent to all parents that they should let us know if there are changed circumstances, or if they want to withdraw permission for their child to be photographed. This reminder will be an annual standing item in a newsletter. Parents retain the right to withdraw consent at any time. The school is obliged to comply with the parents and carers wishes.

2.5 If the two parents/carers disagree over consent for their child to appear in photographs or videos, we shall treat it as if consent has not been given.

2.6 Where children are Looked After the school will gain consent on the corporate parent's behalf via the child/young person's social worker.

3. Getting Consent for adults

3.1 The school will seek written permissions from teachers, support staff, helpers, and volunteers to use their photographs.

4. Planning the use of images

4.1 The school will make sure that people are aware if the school intends to use their photograph in a potentially sensitive publication.

4.2 The school will take care to ensure that only images of students in suitable dress are taken, to reduce the risk of images being used inappropriately. The school will screen all images for acceptability, and if there is any possibility that a photograph could be used inappropriately then it will be destroyed. Particular care will be taken with photographs taken during PE and swimming lessons to maintain modesty.

4.3 No images should be taken of children/young people which capture them in what are commonly understood as non-public activities such as changing clothes or toileting, or which show body parts not usually visible in public settings.

4.4 The school will make sure that photograph shoots are inclusive, showing children/young people from a range of diverse backgrounds and abilities.

4.5 There may be occasions when a child/young person or his/her parent's security is a known risk (i.e., some adoption placements or child resettled after domestic abuse). In such circumstances, a child/young person will not appear in any photograph or image.

5. School plays and other events

5.1 Generally speaking, photograph/video recording will be permitted at school events. The one clear exception to this general rule will be for the congregation at Mass. There may be occasions when the school does not allow photography/video recording. This may be for a variety of reasons, for example:

- Disturbance to other members of the audience
- Distraction to the children taking part in a performance, especially where flash is used.
- Parental objection
- Child protection concerns

5.2 Parents, carers and their families can use photographs and videos taken at a school event for their own personal use. Such photographs and videos cannot be sold and must not be uploaded to the Internet, as that would contravene data protection legislation.

5.3 The school will make all parents/carers aware in advance of the event that other parents may want to video or photograph performances as a record of their child's work or performance.

5.4 The school will make people aware that other parents may be recording the event.

5.5 If an objection is raised, the school shall need to consider ways to overcome this.

6. School fetes and open evenings

6.1 If the school is going to take general shots, at these events, of students and visitors for publicity purposes, the school should warn people in the invitations we send out that this will take place, so that general consent is implied by attendance.

7. Outside Events

7.1 Students may take part in public performances outside the school. In these cases, the event organiser should seek the permission of parents and carers for photographs to be taken and used in publicity.

8. Press Photography and Media Filming

8.1 The media operate under their own Code of Practice.

8.2 Students should not be approached or photographed at school without the permission of the school's authorities, however, we may want to invite the media into school to publicise an event or we may be approached by the media regarding a news story.

8.3 Newspapers will often want to name children in photographs – their first name and surname, and often their age as well. For this reason, it is important that the school makes parents/carers aware of this and give them an opportunity to object to their child being in media photographs.

8.4 If we invite the media into the school for publicity purposes, it is important that we inform parents/carers whose children may feature in photographs or filming.

8.5 If we know there are children who should not be identified as going to the school even if they are in a big group-shoot and are not named, we will need to keep them away from the cameras.

Any school suspecting a person of taking unauthorised photographs, or undertaking unauthorised filming of children, should immediately contact Essex Police.

9. Video Conferencing

9.1 The school will need to explain to parents how this is used and why, and that it means sending images over the internet that might be stored for educational use in schools. If parents/carers have not given permission for internet publication of their child's photograph, the school will need to angle the webcam to avoid these children.

10. Mobile Phones

10.1 Virtually all mobile phones now contain a facility to take photographs and videos and to transmit images taken, including uploading them onto the internet.

10.2 The same rules would apply as for photographs: users need to recognise that any pictures taken are for personal use only. (See guidelines for appropriate use of mobile phones).

11. CCTV

12.6 Where a school has installed closed circuit television (CCTV) as a security measure the school must operate this in accordance with the principles of data protection. Guidance on use can be found in the Trust CCTV Policy.

13. Storage of Images

13.1 All photographs/video recording will be stored in a secure place and is only accessed by people who are authorised to do so. Digital images such as those used for student passes should also be stored securely, including any images stored on CD or other disks and on the school's computer network. Electronic images should be stored on media that is encrypted. The school will take care to ensure that it will not re-use photographs for more than a year after the student leaves the school.

13.2 When the school destroys photographs, it is important to destroy the negatives as well, and in the case of CDs and other media that cannot be erased electronically; the school should render the disk unusable.

14. Risk Assessment for PE and Other School Changing Rooms

14.1 A school risk assessment has been written and put in place to ensure students changing for PE and other changing areas cannot be filmed or pictures taken.

14.2 PE and other relevant staff have read and signed off that they understand the policy.

15. Revision History

Version 1.0	23rd October 2019	Original policy document
Version 1.1	23rd October 2019	Policy Review Addition of version number and header. Addition of revision history (14).
Version 1.2	6th September 2021	Policy Review. No Changes.
Version 1.3	27th October 2022	Policy Review. No Changes.
Version 1.4	8th September 2023	Policy Review. No Changes.
Version 1.5	24th September 2024	Policy Review. Section 12.1 updated from 'Password Protected' to 'Encrypted'.
Version 2.0	25th March 2025	Policy Integration with centralised Online Safety Policy. Replaced introduction references to DVD with Digital. Section 2.4 updated to remove references to 'Contact'. Section 5.4 updated with more succinct language. Section 12.6 updated to reference Trust CCTV Policy.

Appendix G

Use of Mobile Phones and Social Media Policy

The use of mobile phones in the school setting and the procedures for use in place are included within the Trust Online Safety Policy.

1. Staff use of their own personal mobile phone within the school

1.1 Staff, both teaching and support staff are permitted to bring their own mobile phone onto the school premises or on a school related activity out of school.

1.2 Staff are however advised they should not use mobile phones for personal use near students, namely in teaching classrooms, school corridors, or whilst on a formal duty.

1.3 Considerate use of mobile phones is permitted for personal use in the staff room, private offices, out of school hours and when not with students.

1.4 Any school data stored on personal technology should be encrypted. Please refer to 'The ICT Usage and Code of Practice for Staff'.

1.5 Any inappropriate use may lead to disciplinary action.

1.6 Staff bring mobile phones into school at their own risk and should be prudent where they store them when not in use. Storage in teachers' desks in classrooms is not advised.

1.7 In the event that a member of staff is expecting an emergency call, staff should attempt to arrange the call to come through reception and normal channels or to receive the call in private without compromising the duty of care for their students under their supervision at that time.

2. Staff use of work issued mobile phones

2.1 A school mobile may be supplied to group leaders on school trips or outside activities for use in the smooth running of the trip or in the event of an emergency.

2.2 The mobile will, at all times, be kept secure by the group leader or a reliable nominated adult.

2.3 Students should not use a school phone unless supervised for a specific task.

2.4 The emergency school phone number can be given to students and parents for emergency contact purposes.

2.5 If staff elect to store contact numbers for their trip on the school mobile for emergency purposes, the member of staff should delete those numbers once the trip has been completed.

2.6 Confidentiality of the information stored on the mobile phone is secured by the group leader keeping the mobile safe and not accessible to unauthorised users.

2.7 School mobile phones provided to staff for any other purpose should adhere to this guidance.

3. Student use of mobile phones

3.1 Mobile phones should not be brought into school. The decision to provide your child with a mobile phone to give parents/carers reassurance that they can contact their child whilst travelling alone on public transport or journeys to and from school, is made on the understanding that the phone should be switched off completely whilst at school, not merely silenced or on divert or vibrate.

3.2 In order to reduce the risk of theft or loss during the school day, students who carry mobile phones must keep them concealed, not advertise that they have them, and mark them clearly with their name.

3.3 Schools may request that students surrender their mobile phone at a designated location at the beginning of the school day. Mobile phones can be collected by students at the end of the school day.

3.4 During examinations, JCQ guidance will be followed.

3.5 Schools accept no responsibility for replacing mobile phones that are lost, stolen or damaged whilst on or travelling to the school premises, or on school sponsored functions.

3.6 If a student is seen with, or seen using a mobile phone on school premises, the phone will be confiscated to a secure place in school and returned at the end of the school day and a letter will be sent home on a first offence. If a student breaks this rule again, the phone will be confiscated to a secure place in school, parents/carers will be informed who then may collect the phone during office hours. Repeated infringements would be seen as a breach of the Student Behaviour Policy and sanctions may follow.

3.7 It is a criminal offence to use a mobile phone to menace, harass, or offend another person. The school will involve the police if such an event occurs.

4. Parental use of mobile phones in the school

4.1 Parents should not use mobiles whilst in the school setting with the exception of the school reception, sporting events or out of school hours.

4.2 Any concerns related to parental use of mobiles such as volume or content may be raised by members of school staff.

4.3 The use of mobiles to take pictures or video activities is covered under the schools 'Safe use of Images Policy'.

5. Safer use of images guidance

5.1 The school has a 'Safe Use of Images Guidance Policy', which is reviewed and adopted by Governors annually.

5.2 The policy covers who can take photographs with reference to staff, parents, and outside agencies.

5.3 The policy refers to which images cannot be taken.

5.4 A consent form is signed by all parents of students in school who give permission to have their son or daughter photographed. This consent outlines how photographs may be used in the school setting.

5.5 All school photographs are confidentially stored.

5.6 Parental permission for photographs to be taken are logged under student details on SIMS and highlighted in a separate column on the student trip list for each new trip that runs.

5.7 It is expected that the group leader is aware of which students in the group do not have permission for photographs to be taken.

5.8 No student is allowed on a school trip or activity unless the generic consent form has been returned.

6. Use of Social Media networking sites

6.1 Only staff with school authorisation to access specific social media networking sites, may do so.

6.2 Staff accessing social networking sites without authorisation on school equipment may face disciplinary action.

6.3 Staff should not use their personal equipment to access social networking sites in the school setting whilst near students, this includes whilst in the classroom, corridors, computer rooms or other public areas of the school and whilst on duty.

6.4 Appropriate use of electronic technology, using personal equipment may be undertaken in private areas of the school away from the vicinity of the students such as the staff room and offices.

6.5 Inappropriate use of social networking sites either within the school setting or within private time that brings the schools catholic ethos and good name into disrepute could lead to disciplinary action.

6.6 It is prohibited to 'friend' present students at the school on a social networking site such as Facebook unless it has been authorised by the school.

6.7 Staff should refer to the Child Protection and Safeguarding, and Safer Use of Images policies and refer to their terms and conditions of employment to ensure their actions do not bring the schools good name into disrepute.

6.8 Use of electronic technology whether within the school setting or out, should not compromise a member of staffs professional integrity.

7. Revision History

Version 1.0	23rd October 2019	Original policy document
Version 1.1	23rd October 2019	Policy Review Addition of revision history (7). Addition of version number and header. Formatted for easier reference. Headings updated with new terminology.
Version 1.2	6th September 2021	Policy Review. No Changes.
Version 1.3	27th October 2022	Policy Review. No Changes.
Version 1.4	8th September 2023	Policy Review. No Changes.
Version 1.5	24th September 2024	Policy Review Removal of section 2.7 as no longer relevant. Updated section 2.8 to section 2.7 to reference 'all staff'. Updated section 6.8 to reference correct policy names.
Version 2.0	25th March 2025	Policy Integration with centralised Online Safety Policy. Section 3.3 added to include procedures used in primary schools. Section 6.2 updated to remove references to Twitter.

Appendix H

Filtering and Monitoring Policy

Filtering and monitoring systems are used to keep pupils safe when using the school's IT system.

- Filtering systems: block access to harmful sites and content.
- Monitoring systems: identify when a user accesses or searches for certain types of harmful content on school devices (it doesn't stop someone accessing it). The school is then alerted to any concerning content to intervene and respond.

No filtering and monitoring system is 100% effective, so will be used alongside existing safeguarding systems and procedures.

1. Roles and Responsibilities

1.1 All staff should be clear on:

- The expectations, applicable roles, and responsibilities, in relation to filtering and monitoring as part of their safeguarding training. For example, part of their role may be to monitor what's on pupils' screens.
- How to report safeguarding and technical concerns, such as if:
  - They witness or suspect unsuitable material has been accessed.
  - They are able to access unsuitable material.
  - They are teaching topics that could create unusual activity on the filtering logs.
  - There is failure in the software or abuse of the system.
  - There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks.
  - They notice abbreviations or misspellings that allow access to restricted material.

1.2 Senior leaders and all relevant staff need to be aware of and understand:

- What provisions the school has in place and how to manage these provisions effectively.
- How to escalate concerns when they identify them.

1.3 Senior leaders are also responsible for:

- Buying-in the filtering and monitoring system the school uses.
- Documenting what is blocked or allowed, and why.
- Reviewing the effectiveness of the provision, making sure that incidents are urgently picked up, acted on and outcomes are recorded.
- Overseeing reports.
- Making sure staff are trained appropriately and understand their role.

1.4 The DSL should take lead responsibility for online safety, including understanding the filtering and monitoring systems and processes in place, this is part of their role in taking the lead responsibility for safeguarding. This includes overseeing and acting on:

- Filtering and monitoring reports.
- Safeguarding concerns.
- Checks to filtering and monitoring systems.

2. Filtering and Monitoring

2.1 Schools will identify and assign roles and responsibilities to manage filtering and monitoring systems.

2.2 Review filtering and monitoring provision at least annually.

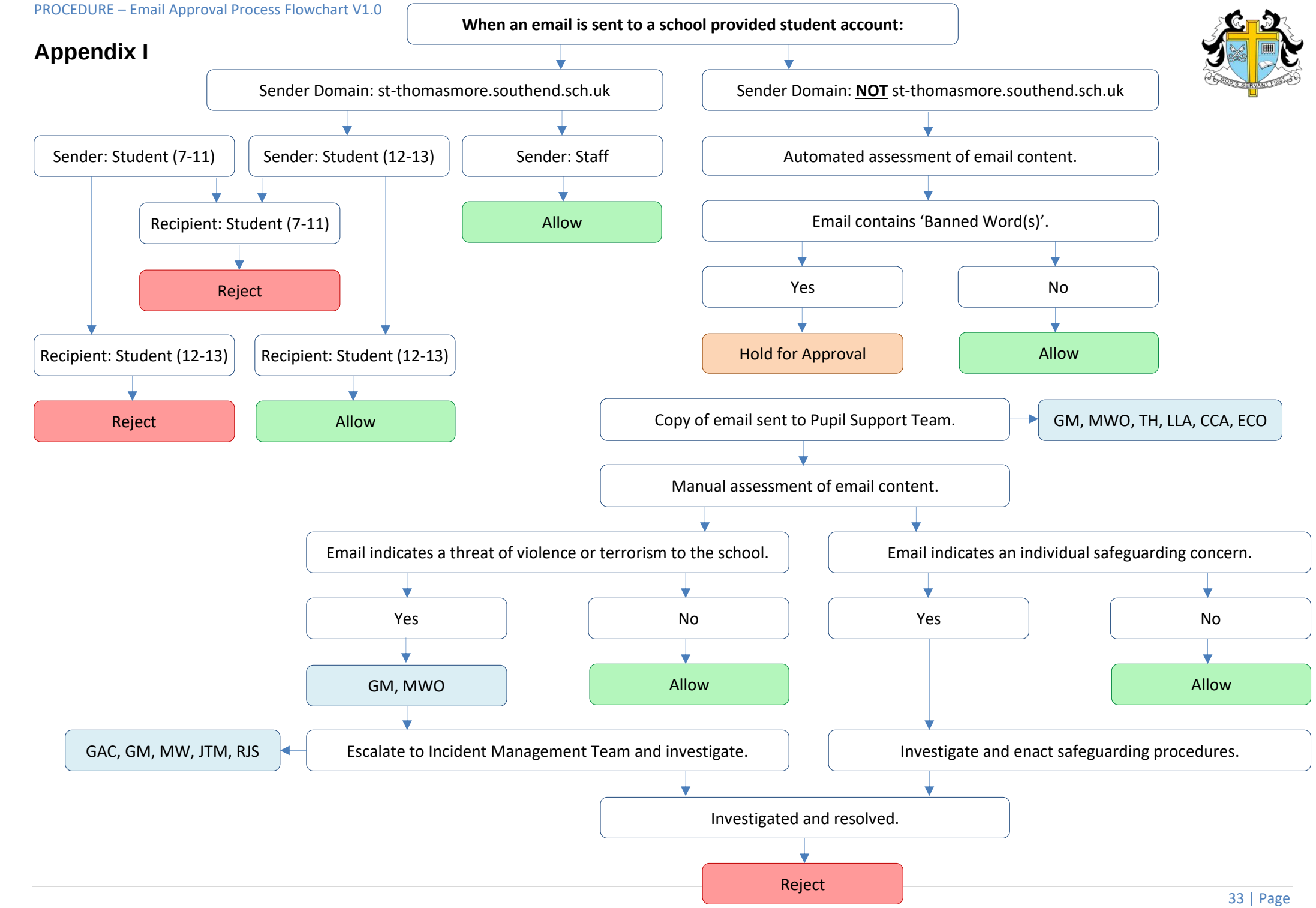
2.3 Block harmful and inappropriate content without unreasonably impacting teaching and learning.

2.4 Have effective monitoring strategies in place that meet safeguarding requirements.

3. Revision History

Version 1.0	8th September 2023	Initial version
Version 1.1	24th September 2024	Policy Review. No Changes.
Version 1.2	26th March 2025	Policy Integration with centralised Online Safety Policy.

Appendix I


When an email is sent to a school provided student account:
Sender Domain: st-thomasmore.southend.sch.uk
Sender Domain: NOT st-thomasmore.southend.sch.uk
Sender: Student (7-11)
Sender: Student (12-13)
Sender: Staff
Recipient: Student (7-11)
Allow
Reject
Automated assessment of email content.
Email contains 'Banned Word(s)'.
Yes
No
Hold for Approval
Allow
Recipient: Student (12-13)
Recipient: Student (12-13)
Reject
Allow
Copy of email sent to Pupil Support Team.
GM, MWO, TH, LLA, CCA, ECO
Manual assessment of email content.
Email indicates a threat of violence or terrorism to the school.
Email indicates an individual safeguarding concern.
Yes
No
Yes
No
GM, MWO
Allow
Allow
GAC, GM, MW, JTM, RJS
Escalate to Incident Management Team and investigate.
Investigate and enact safeguarding procedures.
Investigated and resolved.
Reject