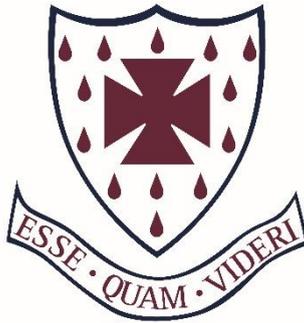# S. Anselm's School

Policy Title: Online Safety Policy

Policy Category: Health & Safety

Policy Number: 19

Policy Owner / Author:	Alison Whawell
Approved by:	Head
Date Approved:	September 2025
Next Review Date:	October 2026
Version:	1.0
Related Policies:	o Anti-bullying Policy o Behaviour Management Policy o Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE) o Data security and GDPR o Safeguarding and Child Protection Policy o Searching, Screening and Confiscation Policy o Staff Code of Conduct o Image use, mobile phone and social media procedures (Staff Handbook)
Confidentiality Label:	⭕ Internal Use Only ⭕ Parent Web Page ⭕ Public Document
Contact for Queries:	

📌 This document is controlled and reviewed as part of the School's policy management process. Please refer to the school's website or Teams to ensure you are using the most up-to-date version.

Enclosures:

Appendix 1: Acceptable Use Policy

Appendix 1A: S. Anselm's School Acceptable Use of ICT for Staff

Appendix 1B**:** S. Anselm's School Acceptable Use of ICT for Pupils

Appendix 2: Safeguarding Children in School

Improving Internet Activity Monitoring for Your Child when using a Bring Your Own Device (BYOD)

This policy links with several other policies and practices including:
o Anti-bullying Policy
o Behaviour Management Policy
o Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE)
o Data security and GDPR
o Safeguarding and Child Protection Policy
o Searching, Screening and Confiscation Policy
o Staff Code of Conduct
o Image use, mobile phone and social media procedures (Staff Handbook)

Contents

1. Policy Aims

● This online safety policy has been written by S. Anselm's School, involving staff, learners and school Governors, building on the Derbyshire County Council online safety policy template, with specialist advice and input, and reformatted including additions. This policy recognises the increasing use of Artificial Intelligence (AI) technologies (e.g. generative AI tools, deepfakes, automated chatbots, recommendation algorithms) and their potential benefits and risks. We will educate and safeguard learners, staff, and parents to critically evaluate AI-generated content, protect personal data, and understand the ethical use of AI.
It considers the DfE statutory guidance 'Keeping Children Safe in Education',2025 Early Years Foundation Stage2025 update, 'Working Together to Safeguard Children' 2015 (with 2025 updates), Meeting Digital and Technology Standards in Schools and Colleges 2022 (with 2024 updates) and the Derby City & Derbyshire Safeguarding Children Board procedures.
● The purpose of this online safety policy is to:
o Safeguard and protect all members of S. Anselm's School community online.
o Identify approaches to educate and raise awareness of online safety throughout the community. o Enable all staff to work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology.
o Identify clear procedures to use when responding to online safety concerns.
● This school identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:
o Content: being exposed to illegal, inappropriate or harmful material
o Contact: being subjected to harmful online interaction with other users
o Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
o Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. (KCSIE 2025).

1.1 Policy Scope
● S. Anselm's School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
● S. Anselm's School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
● S. Anselm's School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
● This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as "staff" in this policy) as well as learners, parents and carers.
● This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.2 Links with other policies and practices
● This policy links with several other policies, practices and action plans including:
This policy links with several other policies and practices including:
o Anti-bullying Policy
o Behaviour Management policy
o Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE)
o Data security and GDPR
o Safeguarding and Child protection policy
o Searching, screening and confiscation policy
o Staff Code of Conduct

o Image use, mobile phone and social media procedures (Staff Handbook)

3. Monitoring and Review

● Technology in this area evolves and changes rapidly. This school reviews this policy at least annually.

● The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

● We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

● To ensure they have oversight of online safety, the *Head teacher and DSL* will be informed of online safety concerns, as appropriate and this will be shared with the Safeguarding Governor as deemed necessary.

● Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

● The Designated Safeguarding Lead (DSL), Alison Whawell, has lead responsibility for online safety. Whilst activities of the Designated Safeguarding Lead may be delegated to an appropriately trained deputy, overall, the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.

● S. Anselm's school recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

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

● Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy and acceptable use policy, which covers acceptable use of technology.

● Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.

● Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.

● Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.

● Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.

● Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. ● Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead (DSL) will:

● Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.

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

● Ensure all members of staff receive regular, up-to-date, and appropriate online safety training including providing staff with resources and CPD on safe and ethical AI use and maintaining current knowledge of AI-related safeguarding risks, including deepfakes, AI-assisted grooming, and misinformation.

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

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

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

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

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

● Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.

● Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.

● Report online safety concerns, as appropriate, to the SLT and Governor in charge of Safeguarding. ● Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.

● Meet regularly with the governor with a lead responsibility for safeguarding.

4.3 It is the responsibility of all members of staff to:

● Contribute to the development of online safety policies.

● Read and adhere to the online safety policy and acceptable use policies.

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

● Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.

● Embed online safety education in curriculum delivery, wherever possible.

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

● Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.

● Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.

● Take personal responsibility for professional development in this area.

- Teach learners to critically evaluate AI-generated content and to avoid sharing personal or sensitive information with AI platforms.
- If using a AI platform we should use Microsoft copilot as it has the largest range of safety features.
- Report suspected misuse of AI technologies, including deepfake images, fake accounts, or algorithm-driven harassment.

4.4 It is the responsibility of staff managing the technical environment to:

● Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.

● Implement appropriate security measures (password procedures and encryption procedures) as directed by the DSL and leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.

● Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.

● Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team

● Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

4.5 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

● Engage in age-appropriate online safety education opportunities.

● Contribute to the development of online safety policies.

● Read and adhere to the acceptable use policies.

● Respect the feelings and rights of others both on and offline.

● Take responsibility for keeping themselves and others safe online.

● Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

• Use only school-approved AI tools (Microsoft copilot) and never share personal details with online AI platforms.

• Report any AI-generated content (e.g., altered images or fake messages) that is harmful, misleading, or offensive.

• Understand that AI outputs may be inaccurate or biased and must be verified.

4.6 It is the responsibility of parents and carers to:

● Read the acceptable use policies (appendix 1) and encourage their children to adhere to them.

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

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

● Abide by the school's acceptable use policy (appendix 1).

● Identify changes in behaviour that could indicate that their child is at risk of harm online. ● Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.

● Use systems, such as learning platforms, (Espresso et al) and other network resources, safely and appropriately.

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

5   Education and Engagement Approaches

5.1 Education and engagement with learners

● The school will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:

o Ensuring education regarding safe and responsible use precedes internet access. o Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.

o Reinforcing online safety messages whenever technology or the internet is in use. o Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.

o Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy, including AI literacy within PSHE, RSE, and computing curricula, covering topics such as misinformation, deepfakes, plagiarism risks, and ethical AI use.

● The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:

o Displaying acceptable use posters in Prep School planners and displaying the is on the splash page of school computers.

o Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.

o Rewarding positive use of technology (through our behaviour policy)

o Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Learners

● S. Anselm's School recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

● S. Anselm's School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.

● When implementing an appropriate online safety policy and curriculum S. Anselm's School will seek input from specialist staff as appropriate, including the SENCO.

5.3 Training and engagement with staff

We will:

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

● Provide up-to-date and appropriate online safety training for all staff on a regular basis.

● Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.

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

● Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.

● Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.

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

5.4 Awareness and engagement with parents and carers

● S. Anselm's School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

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

o Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as information meetings.

o Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.

o Signposting them to read our pupil acceptable use policies and discuss the implications with their children.

• Provide parent briefings on AI trends, risks, and how to discuss them with children, and hare reputable resources on recognising AI-driven scams, fake news, and inappropriate content.

6. Reducing Online Risks

● S. Anselm's School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

● We will:

o Regularly review the methods used to identify, assess and minimise online risks.

o Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.

o Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material. We will collaborate with external experts to stay updated on emerging AI-related threats.

● Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.

● All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could

cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use
● S. Anselm's School uses a wide range of technology. This includes access to:
o Computers, laptops, iPads and other digital devices
o Internet which may include search engines and educational websites
o Learning platform/intranet
o Email
o Digital cameras, web cams and video cameras
● All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
● Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
● The setting will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
● If AI is being used as a learning tool, all pupils should be using Microsoft copilot.
o At S.A all searches default to Google Safe Search, YouTube Safe Search and CBBC Safe Search.
● We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
● Supervision of learners will be appropriate to their age and ability.
    o For Early Years Foundation Stage and Pre-Prep
    ▪ Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
    o Junior Forms
    ▪ Learners sign an AUP (in pupil planners) and receive online safety lessons as part of their coding curriculum.
    ▪ Learners will use age-appropriate search engines and online tools.
    ▪ Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.
    o Prep School
    ▪ Learners sign an AUP ("Using a Computer" in pupil planners) and receive online safety lessons as part of their CCR (Computing, Coding and Robotics) curriculum.
    ▪ Learners will be appropriately supervised when using technology, according to their ability and understanding.
    o Boarding
    ▪ The wide range of after school clubs and activities reduces the access and need for online access, activity, and reliance.
    ▪ When used we will balance children's ability to take part in age-appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe practice by children in accordance with the national minimum standards (NMS).

7.2 Managing Internet Access
● We will maintain a record of users who are granted access to our devices and systems.
● All staff and learners read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.
● Visitors are not given access to our computer system, IT resources, and internet.

● We will carry our regular audits and audit activity to help identify pupils trying to access sites to establish any vulnerabilities and offer advice, support and react accordingly

7.3 Filtering and Monitoring

7.3.1 Decision Making
● S. Anselm's School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
● The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
● Our decision to filter and monitor our internet has been informed by external guidance, considering our specific needs and circumstances.
● Changes to the filtering and monitoring approach will be assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
● The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. This should be done at least annually.
● All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.
● With Addooco we will use the DfE's *'plan technology for your school service'*. This tool can be used to self-assess against the filtering and monitoring standards and receive customised recommendations on how to meet these standards. We will use it to check whether their school security standards are currently fit for purpose.

7.3.2 Filtering
● We work with Addooco to ensure that our filtering policy is continually reviewed.
● The current leased line is through Amvia and is contracted until 19th Sept 2026. It is a 200Mbps circuit on a 1Gbps bearer. Addooco are installing a private 1Gb/1Gb layer 2 connection to the Anselm's datacentre infrastructure. This will be live by December 2025 (install date TBC). At this point, the Amvia connection will be used as a backup only until the end of the contract.
● We use the following internet filtering system; SOPHOS which blocks sites which can be categorised as: Anonymizers, Command & Control, Controlled Substances, Criminal Activity, Download Freeware, Extreme, Gambling, Hacking, Hunting & Fishing, Intellectual Piracy, Intolerance & Hate, Legal Highs, Marijuana, Militancy & Extremist, Newly Registered Websites, Nudity, Peer-to-Peer torrents, Phishing & Fraud, Pro-Suicide & Self-Harm, Sexually Explicit, Spam URLs, Spyware & Malware, Unauthorised Software Stores, Uncategorised, Weapons. Reports are configured in the firewall to notify on Addooco on blocked web attempts.
● The filtering system is supported by and blocks all sites on the Internet Watch Foundation (IWF) list.
● If learners discover unsuitable sites, they will be required to:
o Turn off monitor/screen and report the concern immediate to a member of staff.
o The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff. A ticket will be raised with Addooco so the browser can be added to the block list.
o The breach will be recorded and escalated as appropriate.
o Parents/carers will be informed of filtering breaches involving their child.
o The DSL will ensure that Computing staff are aware in order that they can review the computing curriculum regarding online safety programme.
● Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Derbyshire Police or CEOP.

7.3.4 Monitoring
● We work with Addooco to ensure that our monitoring is effective.
● We will appropriately monitor internet use on all setting owned or provided internet enabled devices, and any privately owned devices to be used by pupils on school premises. This is achieved by:
o Physical monitoring (supervision), monitoring internet and web filtering (SOPHOS).
o Safeguarding Team is responsible for regular monitoring and filtering appropriately any flagged activities through Classroom Cloud.
● If a concern is identified via monitoring approaches we will:
o DSL or deputy will respond in line with the Safeguarding Policy.
● All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online
● Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
o Full information can be found from our Compliance Officer.

7.5 Security and Management of Information Systems
● We take appropriate steps to ensure the security of our information systems, including:
o Virus protection being updated regularly.
o Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
o Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
o Not downloading unapproved software to work devices or opening unfamiliar email attachments.
o Regularly checking files held on our network,
o The appropriate use of user logins and passwords to access our network.
▪ Specific user logins and passwords will be enforced for all but the youngest users. (Note: this should be in place for all except Early Years and Foundation Stage children and some learners with SEND)
o All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password policy
● All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private. Passwords for staff will change every 42 days, in line with ISO27001. We require staff members to use a 'two form factor authentication' to prevent unauthorised access to our systems.
● If using online recording systems e.g. a CP record system, restricted access will be granted per job role and responsibility with regular reviews of who has access
● All learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private. Pre-prep use a 4 digit pin, pupils in Year 3-8 have a 7 digit password: first three characters of their name with one capital and two lower case, a punctuation mark and the year and a question mark: Nam=25? (Name is the first three letters of their name) and this will change each year.
● We therefore require all users to:
o Use strong passwords for access into our system.
o Always keep their password private; users must not share it with others or leave it where others can find it.
o Not to login as another user at any time.
o Change their passwords on a regular basis. Frequency is dependent on the age of the user, with adult users having the greatest password strength and most frequent change.

7.6 Managing the Safety of our Website

● We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).

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

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

● The administrator account for our website will be secured with an appropriately strong password. ● We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

● Where an individual's achievement is celebrated on the website (for example in the news section), first name and initial only will be used. Photo permission is sought from parents, in line with our GDPR policy and this is conducted annually.

7.7 Publishing Images and Videos Online

● We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, pupil parent privacy policy, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

7.8 Managing Email

● Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.

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

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

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

o Setting email addresses and other official contact details will not be used for setting up personal social media accounts.

● Members of the community will immediately tell ICT Manager (sometimes via the form tutor) if they receive offensive communication, and this will be recorded within our safeguarding files/records if appropriate.

7.8.1 Staff email

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

● Members of staff will refer to and adhere to the acceptable use policy and any other policy where staff use of mobiles is referred.

7.8.2 Learner email

● Learners will use provided email accounts for educational purposes.

● Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted. This is included within pupil planners (new from September 2022 and updated annually).

7.9 Educational use of Videoconferencing and/or Webcams

● S. Anselm's School recognise that videoconferencing *and/or* use of webcams can be a challenging activity but brings a wide range of learning benefits. This has been particularly apparent during the required periods of remote learning through the Covid 19 pandemic.

o All videoconferencing *and/or* webcam equipment will be switched off when not in use and will not be set to auto-answer.

o Videoconferencing contact details will not be posted publicly.

o Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.

7.10 Management of Learning Platforms/ On-Line Learning Profiles
● S. Anselm's School uses Tapestry as an on-line learning profile in Pre-prep.
● Leaders and staff will regularly monitor the usage of Tapestry, including message/communication tools and publishing facilities.
● Only current members of staff and parents will have access to the Learning Journey (LJ).
● When staff *and/or* learners leave the setting, their account will be disabled.
● Learners and staff will be advised about acceptable conduct and use when using the LJ.
● All users will be mindful of copyright and will only upload appropriate content onto the LJ.
● Any concerns about content on the LP will be recorded and dealt with in the following ways:
o The user will be asked to remove any material deemed to be inappropriate or offensive. o If the user does not comply, the material will be removed by the site administrator. o Access to the LJ for the user may be suspended.
o The user will need to discuss the issues with a member of leadership before reinstatement. o A learner's parents/carers may be informed.
o If the content is illegal, we will respond in line with existing child protection procedures.
● A visitor (e.g. Inspector or External Local Authority Early Years Improvement Officer) may be invited onto the site by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.
● S. Anselm's has introduced Microsoft Teams, which requires a school email address and password. This is moderated by school staff and Microsoft's security and compliance.

7.11 Management of Applications (apps) used to Record Children's Progress
● We use Tapestry (in EYFS) and iSAMS to track learners' progress and share appropriate information with parents and carers.
● The head is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
● To safeguard learner's data:
o Devices will be appropriately password protected/encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
o All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
o Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

8.1 Expectations
● The expectations' regarding safe and responsible use of social media applies to all members of S. Anselm's School community.
● Members of staff will refer to and adhere to the school's social media procedure and any other policy where the staff use of social media is referred to such as in the Staff Handbook.
● We will control learner and staff access to social media whilst using setting provided devices and systems on site. (*All social media is blocked for learners. The AUP covers staff use and responsibility*)
● Concerns regarding the online conduct of any member of S. Anselm's School community on social media, should be reported to the Head or DSL and will be managed in accordance with our safeguarding, anti-bullying, allegations against staff, behaviour and child protection policies.

- Encourage verification of suspicious images, videos, or messages using trusted fact-checking or reporting mechanisms. Advise staff and learners that AI-generated fake profiles or content can be used for harassment or fraud.

8.2 Learners Personal Use of Social Media

● Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age-appropriate sites and resources. We are aware that many popular social media sites state that they are not for children under the age of 13 and this is part of the computing curriculum.

 ● Any concerns regarding learner's use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

● Learners will be advised:

o To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.

o To only approve and invite known friends on social media sites and to deny access to others by making profiles private.

o Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.

o To use safe passwords.

o To use social media sites which are appropriate for their age and abilities.

o How to block and report unwanted communications.

o How to report concerns both within the setting and externally.

8.3 Official Use of Social Media

● S. Anselm's School official social media channels are:

o Website: https://www.sanselms.co.uk

o Twitter: https://twitter.com/SAnselmsPrep (account name @SAnselmsPrep)

o Facebook: https://www.facebook.com/s.anselms

o Instagram: https://www.instagram.com/sanselmsschool (account name @sanslemsschool)

o Youtube: https://www.youtube.com/@s.anselmsschool8549 (account name @s.anselmsschool8549)

● The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.

o The official use of social media as a communication tool is limited to the official channels above.

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

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

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

o Official social media sites are suitably protected and, where possible, run *and/or* linked *to/from* our website.

o All communication on official social media platforms will be clear, transparent and open to scrutiny.

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

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

o Any official social media activity involving learners will be moderated as far as reasonably possible. (*If appropriate at all*).

● We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels. Microsoft Teams is exempt from this statement due to it being closed to external users for by licence agreement.

● Parents reserve the right to instruct the school does not use images of their child(ren) on official social media channels. This information is listed on the school's educational visit risk assessment and listed in the staffrooms.

9. Use of Personal Devices and Mobile Phones

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

9.1. Staff Use of Personal Devices and Mobile Phones

o Members of staff will refer to and adhere to the school's acceptable use policy and any other policy where the staff use of personal devises and mobile phones is referred to such as the Staff Code of Conduct.

9.2 Learners Use of Personal Devices and Mobile Phones

● S. Anselm's School expects learners' not to use mobile phones unless express permission has been given; mobile phones are to be handed in to the School Office for safe keeping during school hours.

● If a learner needs to contact his/her parents or carers they will be allowed to use a S. Anselm's School phone. Parents are advised to contact their child via the S. Anselm's School office; exceptions may be permitted on a case-by-case basis, as approved by the head teacher.

● If a learner uses a personal device like a laptop for their learning needs, they must gain permission from the Learning Support Department and parents and learners will be asked to sign up to an agreed code of conduct before the device can be used. This code includes having the device monitored by the school's IT Department.

● Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

● Mobile phones and personal devices must not be taken into examinations.

o Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body (ISEB). This may result in the withdrawal from either that examination or all examinations.

● If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.

o Staff may confiscate a learner's device if they believe it is being used to contravene our behaviour or anti-bullying policy or could contain youth produced sexual imagery (sexting).

o Searches of mobile phone or personal devices will only be carried out in accordance with DfE guidance and our policy. (*See* www.gov.uk/government/publications/searching-screening-and-confiscation)

o Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies. (*See* www.gov.uk/government/publications/searching-screening-and-confiscation)

o Mobile phones and devices that have been confiscated will be released to parents or carers. o If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.3 Visitors' Use of Personal Devices and Mobile Phones

● Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: Visitor, Anti-bullying, Behaviour and Safeguarding.

● Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or *head* of any breaches to our policy.

● The visitor sign in system states our visitor guidelines and asks all visitors to acknowledge these.

9.4 Officially provided mobile phones and devices (*Use If provided*)

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

● Setting mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.

● Boarding children are allowed to contact their parents via a school mobile phone. These phones (which are not smart phones and do not have internet access) are held securely in the school office and boarding staff carefully monitor their usage.

● Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

10. Responding to Online Safety Incidents and Concerns

● All members of the school community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

● All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

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

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

● Where there is suspicion that illegal activity has taken place, we will follow the local safeguarding procedures which will include Police using 101, or 999 if there is immediate danger or risk of harm.

● If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL will speak with Call Derbyshire/ Derbyshire Police first to ensure that potential investigations are not compromised.

10.1 Concerns about Learners Welfare

● The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns. The DSL (or deputy) will record these issues in line with our child protection policy.

● The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Derbyshire Safeguarding Children Board thresholds and procedures.

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

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Children

● Our school/ setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" guidance and part 5 of 'Keeping children safe in education' 2025.

● S. Anselm's School recognises that sexual violence and sexual harassment between children can take place online. Examples may include non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.

● S. Anselm's School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

● S. Anselm's School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

● S. Anselm's School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE curriculum.

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

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

● If made aware of online sexual violence and sexual harassment, we will:

o Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.

o If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.

o Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.

o Implement appropriate sanctions in accordance with our behaviour policy.

o Inform parents and carers, if appropriate, about the incident and how it is being managed. o If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.

o If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.

▪ If a criminal offence has been committed, the DSL (or deputy) will discuss this with our local Police first to ensure that investigations are not compromised.

o Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2 Youth Produced Sexual Imagery or "Sexting"

● We will not:

o View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.

▪ If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.

o Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

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

o Act in accordance with our child protection policies and the relevant Derbyshire Safeguarding Child Board's procedures.

o Store the device securely.

▪ If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.

o Carry out a risk assessment which considers any vulnerability of learners involved, including carrying out relevant checks with other agencies.

o Inform parents and carers, if appropriate, about the incident and how it is being managed. o Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

o Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.

o Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.

o Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

▪ Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

o Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

● S. Anselm's School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

● S. Anselm's School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).

● We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.

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

● We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community.

● If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

o Act in accordance with our child protection policies and the relevant Derby and Derbyshire Safeguarding Children Partnership procedures.

o If appropriate, store any devices involved securely.

o Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform our local police via 101, or 999 if a child is at immediate risk.

o Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).

o Inform parents/carers about the incident and how it is being managed.

o Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.

o Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

● We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.

o Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report:

www.ceop.police.uk/safety-centre/

● If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire police by using 101.

● If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Derbyshire police using 101 unless immediate concerns and 999 will be used by the DSL (or deputy).

● If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Derbyshire Police first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

● S. Anselm's School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

● We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

● We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

● If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire Police using 101.

● If made aware of IIOC, we will:

o Act in accordance with our child protection policy and the relevant Derby City & Derbyshire Safeguarding Child Boards procedures.

o Store any devices involved securely.

o Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Derbyshire police or the LADO.

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

o Ensure that the DSL (or deputy) is informed.

o Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .

o Ensure that any copies that exist of the image, for example in emails, are deleted. o Report concerns, as appropriate to parents and carers.

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

o Ensure that the DSL (or deputy) is informed.

o Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .

o Ensure that any copies that exist of the image, for example in emails, are deleted. o Inform the Derbyshire police via 101 (999 if there is an immediate risk of harm) and Children's Services using Call Derbyshire (as appropriate).

o Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police.

o Report concerns, as appropriate to parents and carers.

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

o Ensure that the *head* is informed immediately and without any delay in line with our Managing Allegations against Staff policy.

o Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our Managing Allegations against Staff policy.

o Quarantine any devices until police advice has been sought.

11.5 Cyberbullying

● Cyberbullying, along with all other forms of bullying, will not be tolerated at S. Anselm's School.

● Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

11.6 Online Hate

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

● All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

● The Police will be contacted if a criminal offence is suspected.

● If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Derbyshire police and or the safer Derbyshire website https://www.saferderbyshire.gov.uk/home.aspx

● All Teachers/ staff members must complete regular Prevent Training every two years.

11.7 Online Radicalisation and Extremism

● We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. (*Our existing web filters include extremism and radicalism heuristics)*

● If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy and Derbyshire Prevent pathway which may include a referral into Channel.

● If we are concerned that member of staff may be at risk of radicalisation online, the *head* will be informed immediately, and action will be taken in line with the child protection and allegations policies.

12. Useful Links for Educational Settings

Support and Guidance for Educational Settings

Derby City & Derbyshire Safeguarding Children's Board online procedures DSCB:
● http://derbyshirescbs.proceduresonline.com/

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

LADO
● By referral into Professional.Allegations@derbyshire.gov.uk
● Form found here http://derbyshirescbs.proceduresonline.com/docs_library.html

Call Derbyshire (Starting Point)
● Immediate risk of harm phone 01629 533190
● For all other referrals complete an online form
https://www.derbyshire.gov.uk/social-health/children-and-families/support-for-families/starting-point-referral-form/starting-point-request-for-support-form.aspx
● For professional advice phone 01629 535353

Meeting Digital and Technology Standards in Schools and Colleges
● https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/ Updates
● DfE's *'**plan technology for your school service***'*.

National Links and Resources for Educational Settings
● CEOP:
o www.thinkuknow.co.uk
o www.ceop.police.uk
● Childnet: www.childnet.com
● Internet Matters: www.internetmatters.org

- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - o ChildLine: www.childline.org.uk
  - o Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - o Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers
- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - o www.thinkuknow.co.uk
  - o www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - o ChildLine: www.childline.org.uk
  - o Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

Appendix 1 <u>Acceptable Use Policy</u>

Appendix 1 A

<u>S. Anselm's School Acceptable Use of ICT for Staff</u>

Policy Date: September 2025-2026

Members of staff responsible: Head and DSL

2

Review date: October 2026

ICT (including data) and the related technologies such as virtual classrooms, email, the internet and mobile devices are an expected part of our daily working life in S. Anselm's School. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. Failure to comply could lead to disciplinary action and in severe cases dismissal. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Bursar or Mr P Cook (Head).

1. I will only use S. Anselm's School's email / Internet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.

2. I will comply with the ICT system security (SOPHOS) and not disclose any passwords provided to me by S. Anselm's School or other related authorities.

3. I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

4. I will use school channels ALWAYS (such as school email) when communicating with pupils and with parents on school matters.

5. I will only use the approved, secure email system(s) for any S. Anselm's School business or in exceptional circumstances approved by two from the Head, the Bursar and a Governor.

6. I will ensure that personal data (such as data held by an iSAMs) is kept secure and is used appropriately, whether in S. Anselm's School, taken off S. Anselm's School premises or accessed remotely. Personal or sensitive data taken off site must be encrypted.

7. I will not install any hardware or software without permission of the IT Manager.

8. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

9. Images of pupils and / or staff will only be taken, stored and used for professional purposes in line with S. Anselm's School Safeguarding policy and with written consent of the applicable parent, carer or staff member.

10. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head.

11. I understand that any files / messages stored on S. Anselm's School systems / devices may be removed if deemed inappropriate.

12. I will support S. Anselm's School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the S. Anselm's School community.

13. I will respect copyright and intellectual property rights.

14. I will ensure that my online activity, both in and outside S. Anselm's School, will not bring my professional role or S. Anselm's School into disrepute.

15. I will support and promote S. Anselm's School Online-Safety and Data Security Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

16. I understand that it is my professional duty to read S. Anselm's School's On-line Safety and Data Security Policies and comply with the guidance contained therein.

17. I understand this forms part of the terms and conditions set out in my contract of

employment. **I agree to follow this Code of Conduct and support the safe and secure use of ICT**

throughout the school.

Staff signature _____ **Date** _____

Printed full name_____

Job title _____

S. Anselm's School Acceptable Use of ICT for Pupil Appendix 1B

When children sign into the school system, they need to read the following information, which is a simplified summary of the AUP. The Pupil AUP is also in the pupil planners and has the title 'Using a Computer at S. Anselm's.'

'Using a Computer at S. Anselm's.'

WE WANT TO KEEP YOU SAFE AT S. ANSELM'S SCHOOL AND THIS INCLUDES WHEN YOU USE THE COMPUTERS. WE DO EXPECT YOU TO PLAY YOUR PART IN THIS. MAKE SURE YOU READ THE POINTS BELOW AND YOU MEET OUR CODE OF CONDUCT:

- I will keep my password secret and not let others use my account.
- I will use the computer for the task I have been set.
- I will not share personal information online.
- I will be polite in all messages I send.
- I will be careful not to offend others by my online behaviour.
- I will not use other people's accounts.
- I will not email or chat or text people I do not know.
- I will share with a trusted adult if I am worried about a message or something I see online.
- I will not use or share any images without a teacher's permission.
- I will respect the school firewall and security settings.
- I will only run programmes I am instructed to use by a teacher.
- I will look after and respect the equipment I am using.
- I will only use a personal device when it has been approved and checked by the school's department.
 I will meet this code of conduct.

Name
Signature
Date

Appendix 2 User agreement for a laptop in school

Dear Parents/Carers,

As part of our Bring Your Own Device (BYOD) provision, pupils using laptops in school are expected to follow the school's **BYOD User Agreement**. This helps ensure devices are used responsibly and supportively in lessons.

Please take a moment to read through the key expectations with your child:
- Laptops should only be used during lessons—not at break times.
- When not in use, laptops must be returned to your child's designated locker in Learning Support.
- Pupils must sign laptops in and out each day.
- During teacher input, pupils should close the laptop lid to show they are listening.
- Internet access should only happen with teacher permission.
- Messaging on Teams is only allowed when a teacher has asked pupils to do so.
- Music may only be listened to during work if a teacher gives permission.
- Pupils may email a teacher but only email other students if it's related to schoolwork.
- All typed work should be in font size 12 or 14 and in black.
- Work should be printed at the end of every lesson.
- If printing isn't possible, pupils should save their work to a memory stick and ensure the teacher receives it as soon as possible to stick into their book.
- Learning Support is available to help with printing when needed.

Pupils must follow this agreement to continue using a laptop in school.

Thank you for your support in helping us maintain purposeful and productive learning.

Best wishes,

Mrs Hotston   **Mrs Whawell**

Head of Learning Development   **Deputy Head and DSL**

S. Anselm's School