S. ANSELM'S SCHOOL POLICY

Online Safety Policy

1888

S. Anselm's

Monitoring:	Head
Named Person Responsible:	Alison Whawell
Link Governor:	Katrina Mayson
Designated Safeguarding Lead:	Lisa Donnelly
Reviewed:	February 2020, September 2021
Policy Review Date	September 2022

Enclosures:

Appendix 1: Covid 19

Appendix 2: Online Safety and Etiquette Introduced to Pupils and Parents with the Advent of School Closure March 2020

Appendix 3: Reducing Risks

Appendix 4: Acceptable Use Policy

Appendix 4A: S. Anselm's School Acceptable Use of ICT for Staff

Appendix 4B**:** S. Anselm's School Acceptable Use of ICT for Pupils

Appendix 4C:_AUP for younger children and those with Learning Differences (Simplified Version)

Contents

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.

- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2021, Early Years and Foundation Stage 2021, 'Working Together to Safeguard Children' 2021 and the Derby City & Derbyshire Safeguarding Children Board procedures.

- The purpose of this online safety policy is to:
  - Safeguard and protect all members of S. Anselm's School community online.
  - Identify approaches to educate and raise awareness of online safety throughout the community.
  - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
  - Identify clear procedures to 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 three areas of risk:
  - **Content:** being exposed to illegal, inappropriate or harmful material
  - **Contact:** being subjected to harmful online interaction with other users
  - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

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:
    - Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
    - Anti-bullying policy
    - Behaviour Management policy
    - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE)
    - Data security and GDPR
    - Image use procedures
    - Mobile phone and social media procedures
    - Safeguarding and Child protection policy
    - Searching, screening and confiscation policy

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. This school will review this policy at least annually.
- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the H*ead teacher* will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL), Lisa Donnelly, 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.
- 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.

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.

4.6 It is the responsibility of parents and carers to:

- Read the acceptable use policies (appendix 4) 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 4).
- 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 our systems, such as learning platforms, (Espresso, Digi Maps) 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 setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
  - Reinforcing online safety messages whenever technology or the internet is in use.
  - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
  - Displaying acceptable use posters in all rooms with internet access.
  - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  - Rewarding positive use of technology (through our behaviour policy)
  - Implementing appropriate peer education approaches.
  - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
  - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

    - 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, Child in Care Designated Teacher. (***Head of Learning Support***)

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, with at least annual updates.
- 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:
    - 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 and parent evenings.
    - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
    - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
    - Requiring them to read our acceptable use policies and discuss the implications with their children.

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:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online 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:
    - Computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
    - Learning platform/intranet
    - Email
    - Digital cameras, web cams and video cameras
- The need for remote learning during the Covid 19 pandemic has increased our reliance on the use of technology for learning, especially when we have had remote learning periods.

- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
    - AUP outlines these- e.g. Impero, Smooth Wall, Microsoft Active Directory, Meraki MDM
- 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.
    - 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.
    - **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.
    - **Junior Forms**
        - 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.
    - **Prep School**
        - Learners will be appropriately supervised when using technology, according to their ability and understanding.
    - **College**
        - Learners will be appropriately supervised when using technology, according to their ability and understanding.
        - Learners are expected to BYOD and have laptops at school available for all lessons. They are asked to sign and adhere to the AUP.
    - **Boarding**
        - 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). The wide range of after school clubs and activities reduces the access and need for online access, activity, and reliance.

7.2 Managing Internet Access

- We will maintain a record of users who are granted access to our devices and systems.
- All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or 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 regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- 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.

7.3.2 Filtering

- Education broadband connectivity is provided through Internet Service Providers; Talk Talk, Spitfire and Virgin.
- We use the following internet filtering systems; Smoothwall, Impero for Education and Meraki Networks which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with Smoothwall, Impero for Education and Meraki Networks to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
    - Turn off monitor/screen and report the concern immediate to a member of staff.
    - 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.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.

- 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 will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - Physical monitoring (supervision), monitoring internet and web access (suspect activity is automatically flagged and/or active/pro-active technology monitoring services (Impero and Smoothwall).
- If a concern is identified via monitoring approaches we will:
    - 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.
    - Full information can be found from our Compliance Officer, Mr John Biggin.

7.5 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
    - Regularly checking files held on our network,
    - 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)
    - 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.
- If using online recording systems eg a CP record system restricted access will be granted per job role and responsibility with regular reviews of who has access
- From year 3 (all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
    - Use strong passwords for access into our system.
    - Change their passwords every academic year.
    - Always keep their password private; users must not share it with others or leave it where others can find it.
    - Not to login as another user at any time.
    - Specific user logins and passwords will be enforced for all but the youngest users.
- We require staff members to use a ‘two form factor authentication’ to prevent unauthorised access to our systems.

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.

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

    - Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - Setting email addresses and other official contact details will not be used 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 in 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 to.

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.

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.
    - All videoconferencing *and/or* webcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Videoconferencing contact details will not be posted publicly.
    - Videoconferencing equipment will not be taken off the premises without prior permission from DSL /ICT Department and this should be logged in the school office.
    - 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.
    - Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

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 or transferred to their new establishment.
- 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:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access to the LJ for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement.
    - A learner's parents/carers may be informed.
    - 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 and Show My Homework (March 2020) with the advent of remote teaching and learning has created by the Covid 19 situation. Both Teams (Microsoft Teams) and SMHW (Show My Homework) are accessed through Office 365, which requires a school email address and password. Additionally, SMHW has access for parents, with the primary aim of letting parents know where their children are with work, but this also acts as an additional check. Microsoft Teams is moderated by school staff and Microsoft's security and compliance. More information can be found in Appendix 1 and Appendix 2.

7.11 Management of Applications (apps) used to Record Children's Progress

- We use Tapestry and iSAMS to track learners progress and share appropriate information with parents and carers.
- The *headteacher* 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:
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
    - Devices will be appropriately password protected/encryted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

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 and monitored through web content filtering. 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 DSL and will be managed in accordance with our safeguarding, anti-bullying, allegations against staff, behaviour and child protection policies.

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, therefore we will not create accounts specifically for learners under this age.
- 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:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications.
    - How to report concerns both within the setting and externally.

8.3 Official Use of Social Media

- S. Anselm’s School official social media channels are:
    - https://www.sanselms.co.uk/
    - https://twitter.com/sanselmsprep?lang=en
    - https://en-gb.facebook.com/s.anselms/
    - https://www.youtube.com/channel/UCgecLa6e-ktftyx-zFNUk-A
    - Instagram:@sanselmsschool

- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
    - The official use of social media as a communication tool has been formally risk assessed and approved by the *Marketing Director*.
    - 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.
    - Staff use setting provided email addresses to register for and manage any official social media channels.
    - Official social media sites are suitably protected and, where possible, run *and/or* linked *to/from* our website.
    - 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.
    - Only social media tools that have been risk assessed and approved as suitable for educational purposes will be used.
    - 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.

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

- Members of staff will refer to and adhere to the schools acceptable use policy and any other policy where the staff use of personal devises and mobile phones is referred to.

9.2 Learners Use of Personal Devices and Mobile Phones

- 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.
    - S. Anselm's School expects learners' not to use personal devices and mobile phones unless express permission has been given; these 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 headteacher.
- Personal devices will not be used by learners during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
    - The use of personal devices for a specific education purpose does not mean that blanket use is permitted.
    - If members of staff have an educational reason to allow learners to use their personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- Mobile phones and personal devices must not be taken into examinations.
    - Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. 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.
    - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
    - 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)
    - 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)
    - Mobile phones and devices that have been confiscated will be released to parents or carers.

- 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: anti-bullying, behaviour, child protection and image use.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or *headteacher* of any breaches to our policy. He visitor sign in book does state visitor guidelines.

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

• Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
    - 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.
- We will refer to the flow chart on responding to incidents, made available
- 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. 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" (2018) guidance and part 5 of 'Keeping children safe in education' 2019.
- 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:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - 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.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
    - 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.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2 Youth Produced Sexual Imagery ("Sexting")

- S. Anselm's School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' .
- S. Anselm's School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other 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.
    - 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:
    - Act in accordance with our child protection policies and the relevant Derbyshire Safeguarding Child Board's procedures.
    - Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - 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.
    - Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - 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.
    - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
    - Consider the deletion of images in accordance with the 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.
    - 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:
    - Act in accordance with our child protection policies and the relevant Derby and Derbyshire Safeguarding Children Partnership procedures.
    - If appropriate, store any devices involved securely.
    - 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.
    - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online 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.
    - 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:
  - Act in accordance with our child protection policy and the relevant Derby City & Derbyshire Safeguarding Child Boards procedures.
  - Store any devices involved securely.
  - 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:
  - Ensure that the DSL (or deputy) is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the setting provided devices, we will:
  - Ensure that the DSL (or deputy) is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the Derbyshire police via 101 (999 if there is an immediate risk of harm) and Children's Services using Call Derbyshire (as appropriate).
  - 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.
  - 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:
  - Ensure that the *headteacher* is informed immediately and without any delay in line with our Managing Allegations against Staff policy.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our Managing Allegations against Staff policy.
  - 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

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 *headteacher* 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 Childrens Board on line 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 10629 535353

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - 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
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - 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:
  - www.thinkuknow.co.uk
  - 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
  - ChildLine: www.childline.org.uk
  - 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

Covid – 19

COVID-19 (commonly known as Coronavirus) has presented a huge challenge nationally to the normal running of education and childcare provision. On 23rd March 2020 all schools in the United Kingdom were closed on the advice of the UK Government to help delay the spread of the Coronavirus, and were only to remain open for those children of key workers who could not be safely cared for at home and vulnerable children who need to be cared for in a safe place.

This appendix has been prepared to explain key changes and interim measures being taken within our setting to continue to meet our Online Safety requirements during these extraordinary times and is effective until the School returns to its normal practice of work.

Online Safety during the pandemic of Covid – 19 remains paramount. Whilst the current Online Safety policy should be adhered to there are new arrangements that will need to be considered.

New Online Practices

The advent of remote teaching and learning has created a demand for new online platforms and from March 2020 Microsoft Teams and Show My Homework have been introduced to the S.Anselm's community.

Both Teams (Microsoft Teams) and SMHW (Show My Homework) are accessed through Office 365, which requires a school email address and password. Additionally, SMHW has access for parents, with the primary aim of letting parents know where their children are with work, but this also acts as an additional check.

Personal emails of the pupils or staff are not used.

The introduction of both systems has helped to reduce risk as the sites are username and password protected and come under the ICT services and practices of the school.

Staff and student induction to the systems has included online safety and an online etiquette (for staff at our April 2020 INSET and for pupils with form tutors at the start of term) and code of practice has been shared with pupils, staff and parents and can be referenced in Appendix 2.

Additionally, the safe use of online platforms is discussed at pastoral meetings at staff and year group specific meetings and concerns are dealt with and recorded in Wellbeing Manager or other appropriate records.

Peer – on – Peer abuse / Online safety

With the increased use of social media that will come with the 'lockdown' enabling pupils to keep in touch with their friends, it is essential that pupils are encouraged to report any instances of online bullying or abuse. It is essential that form tutors keep in touch with their tutees during this period and any concerns reported to the Designated Safeguarding Lead or Headteacher. Any reports will be dealt with in line with this and our Safeguarding policy.

Pupils, however, need to be reminded of their behaviour online and this message will be reinforced regularly over the coming weeks and parents will also be sent reminders of what to look out for.

Teachers, parents and pupils will all be provided with a guide to remote learning which will include advice for all users on ‘what to do if..’

The school will investigate the use of online learning tools that can be delivered as part of the online teaching.

Appendix 2

Online Safety and Etiquette Introduced to Pupils and Parents with the Advent of School Closure March 2020

Information conveyed to pupils and their parents in a Handbook at the start of the Remote Teaching and Learning Period in April 2020

WHAT WE EXPECT FROM PUPILS

Behaviour

Pupils represent S. Anselm's School, at all times.

You should show respect and courtesy to others in the school and wider community. You are expected to be honest, display personal and academic integrity, and respect all property.

In the online environment, you are asked and expected to communicate with others in the same way as they would if you were in School.

If you are worried by anything they see, hear or experience online, you should not reply. Pupils should inform a trusted adult about anything upsetting.

Pupil Code of Behaviour for Live Lessons

You should:

- Be ready to start. Your teacher will let you know when to expect the live lesson to start and finish, by giving you the details in SMHW. Try and have all the equipment you need like notebooks, pens and pencils and so on.
- Tell your family you are doing a live session so people can be quiet, free up equipment or Wi-Fi.
- Have the screen fairly upright so that the teacher isn't looking up your nose!
- Wear appropriate clothes. Don't let the teacher know you are still in your pyjamas! We are not expecting you to wear school uniform but do look presentable and school ready.
- Make your learning area quiet, but central. Your bedroom is not the most suitable location.
- Check your background:
- Make sure no one can identify where you live
- Make sure there's nothing unsuitable on the wall
- Make sure family members know that you are online
- We suggest you blur your background. This is an option on Microsoft Teams which your teacher will explain
- Listen to your teacher's instructions, but don't interrupt in the same way you wouldn't in the classroom. Your teacher will start a live session by 'muting' all the class members.
- Your teacher will tell you when they are starting to record the session and also when they are going to finish the recording. This is so some people can catch up later and also if we need to check back on anything if we need to. We expect to only record the teacher and not the pupils.

- If you have a question note these down….and ask them when your teacher tells you. Another way of doing this is typing these into the 'Chat' area of Microsoft Teams. This is a good study skill and one you will have to use more and more as you get older and even enter the world of work.
- Do cooperate with others.
- Be friendly but remember this is a classroom environment - be respectful to the teacher and also your class members.
- Listen to others and don't try to speak over them. Your teacher will use names if they want a contribution.
- Be helpful
- Have good manners
- Treat everyone with respect
- Take responsibility for your own behaviour
- Talk to your form tutor, subject teacher or someone you trust at school or home about anything that worries or concerns you have.
- Remember lessons will be different to what they are like in the classroom but try and be positive. Your teachers are putting a lot of effort into preparing your lessons and your parents are very keen you learn and always try your best.
- Follow this code of behaviour and other rules (including the law)
- Join in and have fun!

You shouldn't:

- Be disrespectful to anyone else
- Bully other people (online or offline)
- Behave in a way that could be intimidating
- Be abusive towards anyone
- Use the chat function for anything other than interacting with your teacher or carrying out a task specifically set by them
- Use the recordings in anyway apart from the way they were intended - simply so pupils can learn and have dynamic lessons.

Appearance

You are not expected to dress formally when working at home. However, the online learning platform is an extension of the classroom, for which pupils are expected to dress appropriately. Staff will remove pupils from a video call if they are dressed inappropriately or are in an inappropriate setting.

Online Safety

Online working is simultaneously easy, informal and open to misinterpretation, especially because of the absence of visual clues. There is always a need to be sensitive to others and to behave appropriately. Remember that people receiving electronic messages may not read them in the tone you intend.

The S. Anselm's School expectations and all other School policies apply when you are working online. It is everyone's duty to model good behaviour online.

It is the School’s

aim to:

- Create a safe and secure environment for children to use technology.
- Have a curriculum in place that ensures the safe and appropriate use of technology.
- Have procedures in place to identify and intervene should any online safety issues arise.

Appendix 3

Risk Reduction

- The school currently does not allow pupils free access to mobile phones throughout the school and laptop computers unless used for Learning Support or for college pupils. This limits risks posed personally via global networks such as the internet.
- There are several secured wireless networks within the school and this means the potential threat to security and access by unauthorised personnel is minimised.
- Pupils access computers, laptops and iPads in the school through secure, password protected connections to the school network.
- Staff have a username and password protected account, with access and allowance limitations imposed.
- The school internet service is firewalled and secured.
- Pupils have controlled internet access.
- Pupils have access monitored via Impero Education Pro software.
- When pupils login on a school device, they receive an internet safety message and rules for use and an agreement.
- Every effort is made to block social networks.
- Users are prevented from downloading executable files.
- All web activity is monitored and personal browsing histories kept by ICT technician
- School web and email settings are set at the highest practicable software security levels.
- The Staff Handbook now covers responsible use of ICT both in and out of school.
- Access to video content on websites is limited and controlled.
- Boarders are allowed internet access for emailing and skype to communicate with home at specific times directed and supervised
- Sexting (the use of mobile devices for the sharing of images of a sexual or indecent nature) is prohibited and procedures are explored in the school's Safeguarding and Child Protection Policy (note appendix 5).
- The school has an Acceptable Use Policy and this is outlined below.

Acceptable Use Policy **Appendix 4**

Appendix 4 A

S. Anselm's School Acceptable Use of ICT for Staff

Policy Date of Policy: July 2021

Members of staff responsible: Headteacher

Review date: July 2022

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 F. Thompson (Headteacher).

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 Headteacher or Governing Body.

2. I will comply with the ICT system security 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 (such as school email) when communicating with pupils ALWAYS 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 data can only be taken out of S. Anselm's School or accessed remotely when authorised by the Headteacher, the Bursar or Governing Body. Personal or sensitive data taken off site must be encrypted.

7. I will not install any hardware of 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 Headteacher.

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 4B**

Online Safety and Etiquette

WHAT WE EXPECT FROM PUPILS

Behaviour

Pupils represent S. Anselm's School, at all times.

You should show respect and courtesy to others in the school and wider community. You are expected to be honest, display personal and academic integrity, and respect all property.

In the online environment, you are asked and expected to communicate with others in the same way as they would if you were in School.

If you are worried by anything they see, hear or experience online, you should not reply. Pupils should inform a trusted adult about anything upsetting.

WHAT YOU CAN EXPECT FROM THE SCHOOL

We believe it is very important for the school to safeguard children and provide technical support while keeping the network secure.

It is the School's aim to:

- Create a safe and secure environment for children to use technology.
- Have a curriculum in place that ensures the safe and appropriate use of technology.
- Have procedures in place to identify and intervene should any online safety issues arise.

As the school regularly updates its ICT facilities, it may be necessary to update BYOD devices to assure compliance. The School Network (which includes all school computers, laptops, tablets, email, virtual learning platforms and Internet access) is owned by the School and is made available to pupils to enhance their own learning. Whilst S. Anselm's school offers access to computers in the Innovation Centre, a student will need to have access to their own device to work from home and/or to bring into the school (BYOD) to use the School Network.

The Acceptable Use Policy (AUP)

The School's Acceptable Use Policy has been drawn up to protect all parties – the pupils, staff and the School.

While using computers, laptops, tablets, email, connected to an online class or the Internet at S. Anselm's School, the rules expected to be followed are:

1. I will use the School's IT facilities with respect and in a responsible manner.

2. I will not use any computer in such a way that would disrupt the computer use of others.

3. I will not attempt to access, edit or delete files or areas belonging to others.

4. I will not interfere with any computer security measures the school may have in place or attempt to bypass the internet filtering system. I will not use a VPN on the school network.

5. I will not connect to the School's IT facilities any device except those expressly permitted by the School.

6. I will not use someone else's username and password to access the computer system, even if they have given me permission to do so.

7. I will not give anyone else my username and password.

8. I will not reveal personal details, address, phone number or password of others, or myself.

9. I will only upload, download or copy files to, or from, the internet with the permission of a member of staff.

10. I will respect copyright and intellectual property rights.

11. I will only use the school printing facilities for printing academic work.

12. I will not attempt to access or download files from the internet or install software, unless instructed to do so by a member of staff.

13. I will ensure that my online activity, both in school and outside school, will not cause others distress or bring the school, its staff or pupils into disrepute.

14. When using email:

- I will report any unpleasant material or messages sent to me. I understand my report will be confidential and would help protect other pupils and myself.
- I will not use bad language or insight bullying in any messages I send.
- I will write emails carefully and politely. As messages may be forwarded, email is best regarded as public property.
- I will not send or forward anonymous letters and chain mail.
- I will be responsible for email I send and for contacts made.

15. I will not use the School's IT facilities to view, download, store, create, share or transmit material which:

- is designed or likely to cause annoyance, inconvenience, needless anxiety or offence;
- is illegal, deceptive or offensive; including defamatory, threatening, abusive or promotes violence, discrimination or extremism;
- infringes copyright (I will not claim the work of another person as my own);
- involves or encourages conduct that promotes illegal activity;
- involves the transmission, distribution or storage of material which breaks any law or seek to harm the School's or others' IT facilities
- I will not click on links unless I am sure of what it is. I will report any dubious web pages and I know these will appear in my history, should I open these.

16. I will report any unpleasant material or messages sent to me. I understand my report will be confidential and would help protect other pupils and myself.

17. I will not access chatrooms, instant messaging, social networking sites or other online email services

18. Images of pupils and / or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of a member of staff.

19. Users should be aware that monitoring and random checks are made on all computer use and all e-mail messages sent and received, and that records are kept. I understand that any files / messages stored on S. Anselm's School's systems / devices may be removed if deemed inappropriate.

20. I will not screen grab, snip or in any way take images of other students or teachers whilst connected to an online classroom.

All rules relating to computer use apply to both computer networks and stand-alone devices in the school. These rules also apply to all information sent electronically within the school, including text messages or pictures sent by mobile phones.

Should any pupil feel upset by either an email or text message in school they can email lisa.donnelly@anselms.co.uk where their concerns will be dealt with in confidence and reports can also be made via this website: www.ceop.gov.uk/

Other useful websites Visit www.thinkuknow.co.uk to ensure you know how to be safe.

PUPIL I have read the rules for Acceptable Computer and Internet Use and know the importance of these rules. I know that if I break these rules, I might lose the right to use the school's computer facilities or face further disciplinary action.

Pupil signature ____

Date ______________________

PARENT/ GUARDIAN I have read the rules for Acceptable Computer and Internet Use and understand that these rules apply when my child is using school computers and the Internet, and all information sent electronically within school. I have gone through the rules with my child and explained their importance and the consequences of breaking the rules.

Parent/Guardian signature ____

Date ______________________

Appendix 4c

AUP for younger children and those with Learning Differences (Simplified Version)

When children sign into the school system, they need to read the following information, which is a simplified summary of the AUP. It is simplified as children from Pre-Prep who are rising twos use the system and this simplified version was felt to better aid their understanding. (Updated September 2021)

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. READ THE POINTS BELOW AND BY PRESSING ENTER, YOU ARE AGREEING TO 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.**