St. Francis' Catholic Primary School
E-Safety Policy

"For it is in giving that we receive."
- St. Francis of Assisi

Key Details

Designated Safeguarding Lead (s): Mrs M Wheeler, Mrs N Fawcett Mrs Lorna Dommett

Named Governor with lead responsibility: Mrs E Hooper

Date written: May 2019

Date agreed and ratified by Governing Body: May 2019

Date of next review: (May 2020)

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Contents

1. Policy Aims

- This E-safety policy has been written by St. Francis' School, building on the Kent County Council (KCC) online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2019.

- The purpose of this policy is to:
    - Safeguard and protect all members of St. Francis' School's 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.

- The 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

St. Francis' school:

- believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.
- identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- believes that pupils 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, 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 pupils and parents/carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school 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 a number of other policies, practices and action plans including:
    - Anti-Bullying policy
    - Acceptable Use Policies (AUP)
    - Behaviour Policy
    - Child Protection Policy
    - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE) Policy
    - GDPR Policy
    - Staff Code of Conduct Policy

2. Monitoring and Review

- The 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 ensure that we 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 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 incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

3. Roles and Responsibilities

- The school has appointed Mrs M Wheeler, as Designated Safeguarding Lead to be the online safety lead.
- The 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 an AUP, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school 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.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- 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 schools 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 management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly (termly) with the governor with a lead responsibility for safeguarding and online safety.

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 AUPs.
- Take responsibility for the security of school 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 school's 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 *(including password policies and encryption)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

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

- Engage in age appropriate online safety education opportunities.

- Contribute to the development of online safety policies.
- Read and adhere to the school AUPs.
- 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 school AUPs and encourage their children to adhere to them.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement and/or AUPs. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school online safety policies.
- 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 pupils

- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including online safety in the PSHE and Computing programmes of study, covering use both at home school and home.
  - Reinforcing online safety messages whenever technology or the internet is in use.
  - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The school will support pupils to read and understand the AUP in a way which suits their age and ability by:
  - Displaying acceptable use posters in all rooms with internet access.
  - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
  - Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
  - Using support, such as external visitors, where appropriate, to complement and support the schools internal online safety education approaches.

5.1.1 Vulnerable Pupils

- The school is aware that some pupils are considered to be 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.
- St. Francis' will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
- St. Francis will seek input from specialist staff as appropriate. Eg. the DSL, SENCO, Child in Care Lead, ELSA.

5.2 Training and engagement with staff

The school will:

- Provide and discuss the Online Safety Policy 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.
    - This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

5.3 Awareness and engagement with parents and carers

- St. Francis' recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school 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 giving reminders about online safety at other events such as assemblies, parent evenings, transition events, fetes and sports days
    - Drawing their attention to the school online safety policy and expectations in newsletters, letters, prospectus and on the website.
    - Requesting that they read online safety information as part of joining the school, for example, within the home school agreement.
    - Requiring them to read and sign the school AUP and discuss its implications with their children.
    -

6. Reducing Online Risks

- St. Francis' School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. The school will:

    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
    - Understand that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.
- All members of the school community are made aware of the school's 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 the school's AUP and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

- St. Francis' School uses a wide range of technology. This includes access to:
    - Computers, laptops, iPads and other digital devices
    - Internet which may include search engines and educational websites
    - Email
    - Digital cameras, web cams?? and video cameras
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place.
- Members of staff will evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.
    - **Early Years Foundation Stage and Key Stage 1**
        - Pupils' 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 pupils' age and ability.
    - **Key Stage 2**
        - Pupils will use age-appropriate search engines and online tools.
        - Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

7.2 Managing Internet Access

- All staff, pupils and visitors will read and sign an AUP before being given access to the school computer system, IT resources or internet.

7.3 Filtering and Monitoring

7.3.1 Decision Making

- St. Francis' School Governors and Leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The Governors and Leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's 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 pupils; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- The school uses educational broadband connectivity through Schools Broadband.
- The school uses the Sophos (Anti-virus) Soft Egg (Filtering System) which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
    - The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- The school works with (Soft Egg/Schools Broadband and Sophos) to ensure that our filtering is continually reviewed.

Dealing with Filtering breaches

- The school has a clear procedure for reporting filtering breaches.
    - If pupils discover unsuitable sites, they will be required to report the concern immediately to the staff member present. The staff member will then minimise the screen.
    - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead 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 that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF (Internet Watch Foundation), Surrey Police or CEOP.

7.3.4 Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
    - P*hysical monitoring (supervision of children on IT equipment & spot checks – history and photos),*
    - *monitoring internet and web access (reviewing logfile information – SoftEgg Reports)*
    - the staff member/s will report issues to the DSL and Senior Management team (SLT
- Concerns identified via monitoring approaches will be reported to Governors and if necessary to appropriate external agencies and parents.
- All users will be informed that use of school 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 the Data Protection Act 1998.
    - Full information can be found in the school's information security policy.

7.5 Security and Management of Information Systems

- The school takes 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 the school's network,
    - The appropriate use of user logins and passwords to access the school network.
        - Specific user logins and passwords will be enforced for all but the youngest users (KS1).
    - 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 school systems; members of staff are responsible for keeping their password private.
- From Year *3* pupils are provided with their own unique username and private passwords to access school systems; pupils are responsible for keeping their password private.
- We require all users to:
    - Use strong passwords for access into our system.
    - Change their passwords every 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.

7.6 Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff and pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

7.7 Publishing Images and Videos Online

- The school will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): the Image use policy, Data security, AUPs, Codes of Conduct, Social Media and Use of personal devices and mobile phones.

7.8 Managing Email

- Access to school email systems will always take place in accordance with data protection legislation and in line with other school policies, including: Confidentiality, AUPs and Code of Conduct.
    - 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.
    - School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell the Head teacher or an SLT member if they receive inappropriate or offensive communication, and this will be recorded in the school safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked in school.
- The school's system for reporting wellbeing and pastoral issues related to emails is to speak to a member of the SLT.

7.8.1 Staff

- The use of personal email addresses by staff for any official school business is not permitted.
    - All members of staff are provided with a specific school email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.

7.8.2 Pupils

- Pupils will use school provided email accounts only for educational purposes.
- Pupils will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9 Educational use of Videoconferencing and/or Webcams

- St. Francis' recognise that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.
    - 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.
    - School videoconferencing equipment will not be taken off school premises without prior permission from the DSL.

- 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.

7.9.1 Users

- Parents and carers consent will be obtained prior to pupils taking part in videoconferencing activities.
- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the pupils' age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, the school will check that recording is permitted to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-school site, staff will check that the material they are delivering is appropriate for the class.

7.10 Management of Learning Platforms

St. Francis' does not currently use a learning platform.

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

- The school uses Target Tracker to track pupils' progress and on occasions may share appropriate information with parents and carers.
- The Head teacher 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
- In order to safeguard pupils data:
    - Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.

- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- School devices will be appropriately encrypted 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 St. Francis' community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of the St Francis' community are expected to engage in social media in a positive, safe and responsible manner, at all times.
    - All members of St Francis 'community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control pupil and staff access to social media whilst using school provided devices and systems on site.
    - The use of social media during school working hours for personal use is not permitted.
    - Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of St Francis' community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Child Protection policies.

8.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of Conduct within the AUP.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are

found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites as strictly as they can.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of St Francis' on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.
    - Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Headteacher.
    - If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

8.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be

raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

- Pupils will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
    - 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 and report concerns both within school and externally.

8.4 Official Use of Social Media

- The St Francis' official social media channel is its Facebook page*.*
- The official use of social media sites, by the school, 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 Headteacher.
    - Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    - Staff use school provided email addresses to register for and manage any official school social media channels.
    - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
    - Official social media use will be conducted in line with existing policies, including: Anti-Bullying, Image use, Data Protection, Confidentiality and Child Protection.

- Parents, carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - Social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
    - Any official social media activity involving pupils will be moderated by the school where possible.
- Parents and carers will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- The school 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.

Staff expectations

- Members of staff who follow and/or like the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
    - Sign the school's Staff Code of Conduct and AUP
    - Be professional at all times and aware that they are an ambassador for the school.
    - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
    - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data Protection and Equalities laws.
    - Ensure that they have appropriate written consent before posting images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
    - Inform their line manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

9. Use of Personal Devices and Mobile Phones

- St. Francis' recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

9.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-Bullying, Behaviour and Child Protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
    - All members of St. Francis' community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
    - All members of St. Francis' community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the school site such as changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community.
- All members of St. Francis' community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour or Child Protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Child Protection, Data security and Acceptable use.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time e.g. locked in a locker/drawer.
    - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
    - Not use personal devices during teaching periods, unless written permission has been given by the Headteacher, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead and/or Headteacher.
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
    - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
    - Directly with pupils, and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches the school policy, action will be taken in line with the Staff Behaviour Code of Allegations Statement and Disciplinary policies.
    - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.3 Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- St. Francis' only allows Y6 to have phones on site. Pupil's personal devices and mobile phones are to be ***switched off*** until the end of the school day and placed in the designated place as directed by the teacher.
- If a pupil needs to contact his/her parents or carers they will be allowed to use a school phone or their phone, under adult supervision, in the school office area.
    - Parents are advised to contact their child via the school office during school hours; exceptions may be permitted on a case-by-case basis, as approved by the Headteacher.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
    - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.

    - If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Senior Leadership Team.
- Mobile phones and personal devices must not be taken into examinations.
    - Pupils 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 pupil's withdrawal from either that examination or all examinations.
- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place.
    - School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Anti-Bullying Policy, or could contain Youth Produced Sexual Imagery (sexting).
    - Pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes school policies.
    - Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the day.
    - If there is suspicion that material on a pupil'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.

9.4 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 the school's Acceptable Use Policy and other associated policies, such as: Anti-bullying, Behaviour, Child Protection and Image use.
- The school will ensure appropriate signage and information is displayed/ 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 Designated Safeguarding Lead of any breaches of school policy.

9.5 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with pupils or parents/ carers is required.
- School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with the Acceptable Use Policy and other relevant policies e.g. Code of Conduct.

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 school procedures for reporting concerns.

    - Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Surrey Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Surrey Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

10.1 Concerns about Pupils Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL will record these issues in line with the school's Child Protection Policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Surrey Safeguarding Children Board thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher, according to the Allegations Statement.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Behaviour Policy and Code of Conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Youth Produced Sexual Imagery or "Sexting"

- St. Francis' recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school 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' and Surrey Safeguarding guidance: "Responding to youth produced sexual imagery".
- St. Francis' 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.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

11.1.1 Dealing with 'Sexting'

- If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:
    - Act in accordance with our Child protection and Safeguarding policies and the relevant Surrey Safeguarding Child Board's procedures.
    - Immediately notify the Designated Safeguarding Lead.
    - Store the device securely.
        - If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
    - Carry out a risk assessment which considers any vulnerability of pupil(s) 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 Specialist Children's Services and/or the Police, as appropriate.
    - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with the school's 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 school 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.
- The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- The school 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.
        - In this case, the image will only be viewed by the Designated Safeguarding Lead 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 children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

11.2 Online Child Sexual Abuse and Exploitation

- St Francis' 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.
- St Francis' recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.
- The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community.

11.2. 1 Dealing with Online Child Sexual Abuse and Exploitation

- If the school are made aware of incident involving online sexual abuse of a child, the school will:
    - Act in accordance with the school's Child Protection and Safeguarding policies and the relevant Surrey Safeguarding Child Board's procedures.
    - Immediately notify the Designated Safeguarding Lead.
    - Store any devices involved securely.
    - Immediately inform Surrey police via 101 (or 999 if a child is at immediate risk)
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Make a referral to Specialist Children's Services (if required/ appropriate).
    - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.
- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
    - Where possible pupils 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 the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Surrey Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Surrey Child Sexual Exploitation Team by the Designated Safeguarding Lead.
- If pupils at other schools are believed to have been targeted, the school will seek support from Surrey Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.3 Indecent Images of Children (IIOC)

- St Francis' will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action 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 (Sophos).
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Surrey Police and/or the Education Safeguarding Team.

- If made aware of IIOC, the school will:
    - Act in accordance with the schools child protection and safeguarding policy and the relevant Surrey Safeguarding Child Boards procedures.
    - Immediately notify the school Designated Safeguard Lead.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Surrey police or the LADO.

- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
    - Ensure that the Designated Safeguard Lead 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 school devices, the school will:
    - Ensure that the Designated Safeguard Lead 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 police via 101 (999 if there is an immediate risk of harm) and children's social services (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 only.
    - 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 school devices, the school will:
    - Ensure that the Headteacher is informed.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
    - Quarantine any devices until police advice has been sought.
    -

11.4 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at St Francis'.
- Full details of how the school will respond to cyberbullying are set out in the Anti-Bullying Policy.

11.5 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at St. Francis' and will be responded to in line with existing school policies, including Anti-Bullying and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Surrey Police.

11.6 Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child Protection Policy.
- If the school is 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.

Useful Links for Educational Settings

Surrey Safeguarding Children Board:
https://www.surreyscb.org.uk/

Surrey County Council Family Information Service:
https://www.surreycc.gov.uk/people-and-community/families/support-and-advice/keeping-your-family-safe/internet-safety

Surrey Police:
https://www.surrey.police.uk

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

National Links and Resources

- 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
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

Appendices

AUP Arrangements:

Parents and children will sign their AUPs as part of the registration process (KS1 or KS2 as appropriate).

In the September of Year 3, the children and their parents will sign the KS2 AUP.

AUPs will be filed in the children's individual files.

New staff will sign the Staff AUP on starting at the school.

Visitor Volunteers (including students) will sign the AUP as they start helping.

St. Francis' Catholic Primary Caterham

"For it is in giving that we receive." - St. Francis of Assisi

KS1 Acceptable Use Agreement

Be Safe Online

S 	**See and tell.** I will only use the computers and iPads with an adult present and if I see something I don't like on a screen, I will always tell an adult.
A 	**Always keep details safe.** I will not tell anyone my passwords, name address or telephone number because I know that people online may pretend to be my friend but could be strangers instead.
F 	**Friendly and polite.** I will only send friendly and polite messages. I will not send anything that would upset or harm someone.
E 	**Extra care online.** I know the school can see what I am doing online. I will only click on safe icons and links that my teacher allows.

If I break the rules, I may not be able to use the computers and iPads.

I have read and talked about these rules with my parents/carers. I can visit www.thinkuknow.co.uk to learn more about staying safe online.

My Name:

Parent's/Carer's signature:

"For it is in giving that we receive."
- St. Francis of Assisi

KS2 Acceptable Use Agreement

Stay Safe Online

I understand that I must use school computing systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the computing systems and other users. I understand that the school may check my computer files and the internet sites I visit.

Keeping safe:

- I will keep my logins and passwords safe and secure - I will not share them with anyone.
- I will never try to find out or use any other person's logins or passwords.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will be aware of "stranger danger" when I am communicating on-line
- If someone suggests meeting up, I will immediately tell an adult.
- **If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it, but I will show a teacher / responsible adult.** I will minimise the page or turn off the screen.
- I will not disclose or share personal information about myself or others when on-line (this includes photos, videos, names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will ask permission before opening an email from someone I don't know, downloading internet files and opening attachments.

Responsible behaviour:

- I will only use the school's computers for schoolwork and will ask permission from an adult before using the internet.
- I will only use my mobile phone if allowed to do so by a teacher.
- I will only edit or delete my own files and not look at, or change, other people's files.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I will only e-mail people I know, or a responsible adult has approved.
- I will only post pictures or videos if they are appropriate and if I have permission.
- The messages I send, or information I upload, will always be polite, sensible and appropriate.
- I will not post any content, comments, images or videos which could cause harm, distress or offence to members of the community.
- I know that information on the internet is not always reliable and that there are laws to stop me using online content without crediting the person or source.

Caring for:

- I will report any damage to equipment to a teacher however this may have happened.
- I will treat all the computing equipment with respect and handle it carefully.
- I will report anyone being unsafe with technology to my teacher.I understand that if I fail to comply with this Acceptable Use Agreement I will be disciplined in line with the school behaviour policy. This may include loss of break times, contact with parents and, in the event of illegal activities, involvement of police.

I have read and talked about these rules with my parents/carers.

I can visit www.thinkuknow.co.uk to learn more about staying safe online.

My signature:

Parent's/Carer's signature:

Parent/Carer Acceptable Use Policy Agreement

(For detailed information on keeping children safe online, please visit www.ceop.gov.uk/ and www.thinkuknow.co.uk/ . To see the school's e-safety policy, please visit the school's website.)

The Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to Computing to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Permission Form

I give permission for my son / daughter to have access to the internet at school and the school's email system, IT systems and equipment.

I have supported my child in signing an Acceptable Use Agreement and know they will receive e-safety education to help them understand the importance of safe use of IT, both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the IT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I understand that if my child does not abide by the Acceptable Use Policy, then sanctions will be applied in line with the school policies, including behaviour, online safety and anti-bullying policies. If the school believes that my child has committed a criminal offence, then the Police may be contacted.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety. I know I can speak to the Designated Safeguarding Lead, my child's teacher or the head teacher if I have any concerns about online safety.

I, together with my child, will support the school's approach to online safety and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community. I support the school's 'use of digital images and videos' policy. I will not take and share online, photographs of other children (or staff) at school events without permission, e.g. on Facebook, Messenger, SnapChat, Instagram etc. I know that I can speak to the school Designate Safeguarding Leads (Mrs MWheeler, Mrs N Fawcett and Mrs L Dommett), my child's teacher or the Headteacher if I have any concerns about safety online.

Pupil Name:	Parent/Carer's Signature	Date:

Staff Acceptable Use Agreement

At St Francis, we recognise that staff can be vulnerable to online risks. Social media can blur the definitions of personal and working lives; it is important that all members of staff at St. Francis' take precautions in order to protect themselves both professionally and personally online. With this in mind, we request that all members of staff adhere to the terms of this agreement as detailed below. This agreement covers the use of digital technologies in school: i.e. **email, Internet, intranet and network resources,** software, data and data storage, **digital cameras, systems, website (including blogs) and social media.**

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it. (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word, is only used on one system and is changed regularly.)
- I will log off the network when leaving a workstation unattended.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols, including GDPR. I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system and Google Drive account (where agreed) for any school business.
- I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive or harmful to colleagues or other members of the school community.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the E Safety Co-ordinator.
- I will not download any software or resources from the Internet or any hardware without the permission of the system manager, in case they can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other IT 'defence' systems.
- I will scan USB devices for viruses before using. (See Computing Co-ordinator for information on how to do this.)
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will keep my mobile phone out of sight of the pupils during working hours i.e. in a cupboard or desk.

- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I will take steps to ensure that my personal information and content is not accessible to anybody who does not or should not have access to it.
- I will ensure that the privacy settings of the social media sites are use are set appropriately and that access is restricted.
- I will not accept pupils (past of present) or their parents / carers as 'friends' on a personal account. (Where there is a pre-existing relationship that may compromise this or if you have any queries or concerns, please speak to the Designated Safeguarding Lead (Lorna Dommett).
- I understand that when using any social networking I am required to uphold the reputation of the school, maintain reasonable standards in my behaviour and uphold the public trust in the profession. I will not do anything that will bring the school into disrepute.
- I will not mention children's names whilst using the School WhatsApp Group and will use this system primarily for conveying work-based messages and information, rather than for socialising.
- I will not use children's names on the class blog and will be mindful of copyright.
- I will password protect my phone and devices if using these for accessing school emails and WhatsApp.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will protect the devices in my care from unapproved access and theft.
- I will access school resources remotely only through the school approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching, including on-line safety/digital literacy and counter extremism and will encourage pupils to report issues that arise.
- I will alert the school's named child protection officer if I feel the behaviour of any child I teach may be a cause for concern.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage and network usage can be logged and this information could be made available to the SLT on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / Designated Safeguarding Lead at the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.

I agree to abide by all the points above. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent E-Safety and Staff Behaviour Code of Conduct, Disciplinary and Facebook policies.

Name: …….. Signature……..Date……..

Job title .....

(Further information is available at the CEOP, NSPCC, childnet, e-safety.org, saferinternet.org and ThinkuKnow websites.)

Visitor/Volunteer Acceptable Use Agreement

As a professional organisation with responsibility for children's safeguarding, it is important that all members of the community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy. This is not an exhaustive list and visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with Data Protection legislation, including GDPR. Any data which is being removed from the school site, such as via email or on memory sticks or CDs, will be encrypted by a method approved by the school.

2. I have read and understood the school E-Safety Policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

3. I will follow the school's policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times.
    - All communication will take place via school approved communication channels such as via a school provided email address or telephone number and not via personal devices or communication channels such as via personal email, social networking or mobile phones.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead (Lorna Dommett) and/or Headteacher.

5. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law.

6. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

7. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

8. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Leads (Maria Wheeler Headteacher, Lorna Dommett DSL & SENCO or Nanda Fawcett DSL & Deputy).

9. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Leads (Maria Wheeler Headteacher, Lorna Dommett DSL & SENCO or Nanda Fawcett DSL & Deputy).

10. I understand that if the school believes inappropriate use or unacceptable behaviour is taking place, the school may invoke its disciplinary procedure. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with the St. Francis' Visitor /Volunteer Acceptable Use Agreement. Signed: …….... Print Name: …… Date: ……

Accepted by:……. ……Date: ……..