

ST FRANCIS OF ASSISI CATHOLIC PRIMARY SCHOOL



ONLINE SAFETY POLICY

Mission Statement



*Compassion – We love and care
Humility – We put others first
Responsibility – We do what is right
Inspiration – We love to learn and achieve
Solidarity – We stand together
Truth – We live by God's Word*

Context

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

The staff and governors of St. Francis of Assisi recognise they have a duty to ensure that all pupils are able to make a valuable contribution to society and this is only possible to achieve if we ensure that pupils develop and apply their ICT capability effectively in their everyday lives.

The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure. There are relevant and comprehensive policies in place which are understood and adhered to by network users.

It is the duty of the school to ensure that every child in their care is safe, and the same principles apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties - the pupils, staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements of school policy.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet and AI
- Mobile phones
- Digital cameras
- e-mail
- Instant messaging
- Web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive Online education programme for pupils, staff and parents.

Roles and Responsibilities

Online safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of governing body, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The e-Safety Coordinators are Hayley Wadie and Beth Hatton and the Computing Lead is Arthe Suluskan.

Online Safety Coordinator/Computing Leader

Our e-safety Coordinators ensure they keep up to date with Online issues and guidance through liaison with the Local Authority Online Officer and through organisations such as WSGFL & Child Exploitation and Online Protection (CEOP). The Headteacher and safeguarding team take day to day responsibility for Online issues. The e-safety Coordinators provide training and advice for staff and monitor the teaching of the e-safety curriculum.

The e-Safety Coordinators:

- Leads the Online Safety Group;
- Take a leading role in establishing and reviewing the school Online Safety policies/documents;
- Work with SLT to ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place;
- Provides training and advice for staff, pupils and parents;
- Liaises with the Local Authority, as necessary, following consultation with the Head Teacher;
- Liaises with school technical staff as necessary;
- Completes and maintains the 360 e-safety review and certification.
- Supports the Digital Leaders to create newsletter updates and collect pupil voice.

Headteacher/Designated Safeguarding Leads

- The Headteacher and other designated safeguarding leads, have a duty of care for ensuring the safety (including Online Safety) of members of the school community.
- Receives reports of Online Safety incidents and creates a log of incidents to inform Future Online Safety developments.

St Francis of Assisi Catholic Primary School Online Policy

- The Headteacher and other designated safeguarding leads should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff. (see flow chart on dealing with Online Safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR disciplinary procedures).
- The Headteacher and other designated safeguarding leads should be aware of the procedures to be followed in the event of a serious Online Safety allegation, linked to the Prevent agenda and how to refer concerns to Channel.
- The Headteacher/safeguarding leads are responsible for ensuring that all other staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Headteacher/ safeguarding leads will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Computing Subject Leader and/or e-safety Leads.

Full Governing Board

The FGB have an overview understanding of Online issues and strategies at this school. The Online coordinator will update the governing body at least once a year to ensure that the FGB are aware of changes in local and national guidance. A member of the FGB (Sue Faulkner) has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- Regular meetings with the Computing/e-safety Leads;
- Regular monitoring of the Online Safety incident logs;
- Regular monitoring of filtering/change control logs;
- Reporting to the relevant Governors during meetings.
- A Governor representative to attend the Online Safety Group.

Teaching Staff and Support Staff

All teachers:

- are responsible for promoting and supporting safe behaviours in their classrooms and following school online procedures.
- are responsible for ensuring online issues are embedded in all aspects of the curriculum and other activities.
- Are responsible for teaching Project Evolve e-safety lessons each term.

All staff are responsible for ensuring:

- They are familiar with the schools' Online Safety policy and practices including:
 - Safe use of e-mail;

St Francis of Assisi Catholic Primary School Online Policy

- Safe use of Internet including use of internet-based communication services, such as instant messaging and social networking;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of pupil information/photographs and use of website;
- eBullying / i procedures;
- Understand their role in providing Online education for pupils;
- They report any misuse or problem to the Headteacher/Senior Leader for investigation/action.
- They monitor the use of digital technologies, mobile devices, and cameras in lessons and other school activities and implement current policies with regard to these.
- In lessons where internet use is pre-planned, students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Staff are reminded / updated about online matters at least once a year.

Senior designated safeguarding leads

The senior designated safeguarding leads should be trained in Online Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data;
- access to illegal/inappropriate materials;
- inappropriate on-line contact with adults/strangers;
- potential or actual incidents of grooming;
- potential or actual incidents linked to radicalisation;
- cyber-bullying.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community. Members of the Online Safety Group will assist the e-safety and Computing Leads with:

- the production/review/monitoring of the school Online Safety policy/documents;
- requests for filtering changes;
- consulting parents/carers and the students/pupils about the Online Safety provision;
- monitoring improvement actions identified through use of the 360 degree safe self-review tool;
- Enabling parents and children to have a voice.

(Appendix B - An Online Safety Group Terms of Reference)

The IT Network Manager (JSPC)

The IT Network Manager is responsible for ensuring:

St Francis of Assisi Catholic Primary School Online Policy

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets required online technical requirements and any Local Authority Online Policy/Guidance that may apply;
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (See Appendix F);
- that they keep up to date with Online technical information in order to effectively carry out their Online role and to inform and update others as relevant;
- that the use of the network/internet/remote access /email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Senior Leader/Online Coordinator for investigation /action;
- that monitoring software/systems are implemented and updated as agreed in school policies.

Students/Pupils

The school includes online education in both the EPR curriculum and the Computing curriculum through Project Evolve and Safer Internet Day. Every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem. They are also taught how to keep passwords and personal information safe. Students are:

- Responsible for using the school digital technology systems in accordance with the Student/Pupil Acceptable Use Policy;
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should know and understand policies on the taking/use of images on cyber-bullying;
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the School's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

The school engages with parents in relation to online safety, and provides education sessions yearly. The school takes every opportunity to help parents understand how they can help in educating their children in how to stay safe through parents' evenings, newsletters, letters and the school's website. Parents and carers will be encouraged to support the school in promoting good online practice and to follow guidelines on the appropriate use of:

- Digital and video images taken in school events;
- Talking to their children at home about how to stay safe online.

Communications

How will the policy be shared?

The policy is reviewed yearly and shared with staff. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding. Induction of new staff includes a discussion of the school's Online Safety Policy. The Policy is also available on the website for other parties.

How will parents' support be enlisted?

The school is able to help parents plan appropriate supervised use of the internet at home by:

- Encouraging a partnership approach which includes:
 - Providing a yearly parent workshop with demonstrations and suggestions for safe home Internet use;
 - Parent representation on the online safety group.
 - Providing a designated online area on our website about e-safety.
 - Providing references to relevant websites/publications e.g. www.safertinternet.org.uk, <http://childnet.com/parents-and-carers>, and <https://www.thinkuknow.co.uk>.
 - Ensuring that Internet issues will be handled sensitively, and parents will be advised accordingly.

How will complaints regarding online safety be handled?

The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];
- referral to LA / Police.



St Francis of Assisi Catholic Primary School Online Policy

Our DSLs acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Managing the Internet Safely

Managing AI safely:

The school will educate pupils on AI through our e-safety curriculum and maintain safe use of AI. Please refer to separate AI policy.

Technical and Infrastructure:

The school has a managed ICT service provided by an outside contractor (JSPC). It is important that the managed service provider is fully aware of the school's Online Safety Policy/ Acceptable Use Agreements.

This school:

- Maintains the filtered broadband connectivity through Exa networks;
- Works in partnership with the LA to ensure any concerns about the system are communicated to WSGfL so that systems remain robust and protect pupils;
- Utilises caching as part of the network set-up;
- Ensures the Systems Administrator / network manager is up-to-date with WSGfL services and policies;
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows pupils access to Internet logs;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Never allows personal level data off-site unless it is on an encrypted device;
- Uses 'safer' search engines with pupils where appropriate, e.g. Kiddle

Policy and Procedures:

This school:

- Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;

St Francis of Assisi Catholic Primary School Online Policy

- We use the Exa Networks SurfProtect filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature (see Appendix F);
- Uses eSafe software to monitor pupils' and staff's use of the internet and software on the computers. A weekly report of infringements and misuse is sent to the Head Teacher.
- Staff preview all sites before use, where not previously viewed and cached.
- Plans the curriculum context for Internet use to match pupils' ability, using child friendly (Kiddle) search engines where more open internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs users that Internet use is monitored;
- Informs staff and pupils that they must report any failure of the filtering systems directly to the IT Network Manager (JSPC). Our systems administrators report to LA / WSGFL where necessary;
- Only uses approved or checked webcam sites;
- Keeps a record, e.g. print-out, of any online bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities, including the Police and the Local Authority.

Education and training:

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse;
- Reinforces key online safety messages in a planned programme of assemblies and class activities;
- Ensures that students understand the need for the Acceptable Use Agreement and are encouraged to adopt safe and responsible use both within and outside school;
- Has a clear, progressive online safety education programme throughout the curriculum all Key Stages, using Project Evolve. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
 - to STOP and THINK before they CLICK;

St Francis of Assisi Catholic Primary School Online Policy

- to discriminate between fact, fiction and opinion;
- to develop a range of strategies to validate and verify information before accepting its accuracy;
- to skim and scan information;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know some search engines / web sites that are more likely to bring effective results; to know how to narrow down or refine a search;
- to understand how search engines work;
- to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files - such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;

Copyright and Plagiarism:

This school:

- ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on- line gaming / gambling;
- ensures staff know how to encrypt data where the sensitivity requires and that they understand data protection and general ICT security issues linked to their role and responsibilities;
- makes training available to staff on the Online education program;
- runs a rolling programme of advice, guidance and training for parents, including:
 - information in school newsletters and on the school web site;
 - demonstrations, practical sessions held at school;
 - suggestions for safe Internet use at home;

St Francis of Assisi Catholic Primary School Online Policy

- provision of information about national support sites for parents.

1. Managing e-mail

E-mail is now an essential means of communication for staff in our schools and increasingly for pupils and homes.

This school:

- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for any communication with the wider public;
- Staff only use work emails for work related communication.
- Contacts the police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law;
- Manages accounts effectively, with up to date account details of users;
- Reports messages relating to or in support of illegal activities;

2. Use of Digital and Video images

In this school:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to the website team;
- The school web site complies with the school's statutory requirements;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities is not published;
- Photographs published on the web do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year - unless an item is specifically kept for a key school publication;
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Pupils are taught about how images can be abused in their online safety education programme.

3. Social Media – Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training, to include acceptable use, social media risks, checking of settings, data protection and reporting issues;
- Clear reporting guidance, including responsibilities, procedures and sanctions;
- Risk assessment, including legal risk.

School staff should ensure that:

- no reference should be made in social media to students/pupils, parents/carers or school staff;
- staff do not engage in online discussion on personal matters relating to members of the school community;
- personal opinions are not attributed to the school or local authority;
- security settings on personal social media profiles are regularly checked, to minimise risk of loss of personal information.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

4. Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- kept no longer than is necessary;
- processed in accordance with the data subject's rights;
- secure;
- only transferred to others with adequate protection.

The school must ensure that:

- it will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for;
- every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay;
- all personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". Please see the Freedom of Information publication hosted on the school's website;
- it has a Data Protection Policy;
- it is registered as a Data Controller for the purposes of the Data Protection Act (DPA);
- responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs);
- risk assessments on IT are carried out and are kept up to date;
- it has clear and understood arrangements for the security, storage and transfer of personal data;
- data subjects have rights of access and there are clear procedures for this to be obtained;
- there are clear and understood policies and routines for the deletion and disposal of data;
- there is a policy for reporting, logging, managing and recovering from information risk incidents;
- there are clear Data Protection clauses in all contracts where personal data may be passed to third parties;
- there are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:



St Francis of Assisi Catholic Primary School Online Policy

- at all times, take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data;
- transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be password protected;
- the device must be password protected;
- the device must offer approved virus and malware checking software;
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

8. Managing equipment

The computer system / network is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely this school:

- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins - these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user - if two people log on at the same time this may corrupt personal files and profiles;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended. Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
- Maintains equipment to ensure Health and Safety is followed;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to security.

5. Responding to incidents of misuse

Please refer to Safeguarding Policy.

6. Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group made up of:

- Senior Leaders;
- E-safety Leaders;
- Online Safety Group

Schedule

This Online Safety Policy was approved by the FGB.	<i>Insert date here</i>
The implementation of this Online Safety policy will be monitored by the:	Senior Leadership Team
Monitoring will take place at regular intervals in line with safeguarding.	
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:	Summer 2026.

The school will monitor the impact of this policy using:

- Logs of reported incidents;
- Monitoring logs of internet activity (including sites visited);
- Internal monitoring data for network activity;
- Surveys/questionnaires of pupils, parents/carers, staff.

Appendix A:

Online Safety Group Terms of Reference

1. PURPOSE

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding Online Safety and the monitoring the Online Safety policy including the impact of initiatives.

2. MEMBERSHIP

2.1 The Online Safety group will seek to include representation from all stakeholders.

The composition of the group should include:

- SLT member;
- Teaching staff member;
- Support staff member;
- Online Safety & Computing Leader;
- Governor;
- Pupil representation – for advice and feedback. Pupil voice is essential in the makeup of the Online Safety group, but pupils would not take part in meetings.
- Parents.

2.2 Other people may be invited to attend the meetings, at the request of the Chairperson on behalf of the committee, to provide advice and assistance where necessary.

2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve them or members of their families.

2.4 Committee members must be aware that some issues discussed by this group could be of a sensitive or confidential nature.

2.5 When individual members feel uncomfortable about what is being discussed, they should be allowed to leave the meeting, with steps being made by other members to allow for these sensitivities.

3. DURATION OF MEETINGS

Meetings shall be held twice a year.

4. FUNCTIONS

These are to assist the Online Safety Coordinator with the following;

- To keep up to date with new developments in the area of Online Safety;
- To annually review and develop the Online Safety policy in line with new technologies and incidents;
- To monitor the delivery and impact of the Online Safety policy;



St Francis of Assisi Catholic Primary School Online Policy

- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of Online Safety. This could be carried out through:
 - staff meetings;
 - pupil forums (for advice and feedback);
 - governors meetings;
 - surveys/questionnaires for pupils, parents/carers and staff;
 - parents' evenings;
 - website/Newsletters;
 - online Safety events;
 - Internet Safety Day (annually - held on the second Tuesday in February).

5. AMENDMENTS

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority.

The above Terms of Reference for St Francis of Assisi Catholic Primary School have been agreed

Signed by (SLT):

Date:

Date for review:

Appendix B:

Staff Acceptable Use Agreement



St Francis of Assisi Catholic Primary School Online Policy

Staff User Agreement Form for the Staff Acceptable Use Policy

As a school user of the network resources, I agree to follow the school expectations as set out in the Online Safety Policy. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the Headteacher.

I agree to report any misuse of the network to the Headteacher.

I also agree to report any websites that are available on the school Internet that contain inappropriate material to the Headteacher.

Lastly I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to SLT.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Staff Name: _____

Staff Signature (if appropriate): _____

Date: __/__/____

Appendix C: Handling of infringements

Record onto CPOMS

Pupils

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging / social networking sites.

Category A sanctions

- Referral to Key Stage leader or member of the leadership team.

Category B infringements

- Continued use of non-educational sites during lessons after being warned;
- Continued unauthorised use of email after being warned;
- Continued use of unauthorised instant messaging / chat rooms, social networking sites, Newsgroups;
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it.

Category B sanctions

- Referral to Headteacher or deputy head teacher;
- Removal of Internet access rights for a period;
- Contact with parent.

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others;
- Sending an email or message that is regarded as harassment or of a bullying nature (one-off);
- Deliberately trying to access offensive or pornographic material;
- Any purchasing or ordering of items over the Internet;
- Transmission of commercial or advertising material.

Category C sanctions

- Referral to Headteacher or deputy head teacher;
- Referral to Online coordinator;
- Removal of internet rights for a more extended period;



St Francis of Assisi Catholic Primary School Online Policy

- Contact with parents.

Other safeguarding actions:

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Referral to Headteacher or deputy head teacher.

Category D infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

Category D sanctions

- Referred to Headteacher;
- Contact with parents;
- Possible exclusion;
- Refer to Community Police Officer;
- LA Online officer.

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

Staff**Category A infringements (Misconduct)**

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the world wide web that compromises the staff members' professional standing in the school and community.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

[Sanction - Referred to Headteacher / FGB and follow school disciplinary procedures; Discuss with HR advisor, report to Police]

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.



St Francis of Assisi Catholic Primary School Online Policy

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Human Resources Advisor.

Child Pornography

In the case of Child Pornography being found, the member of staff should be immediately suspended and the Police should be called. Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP).



St Francis of Assisi Catholic Primary School Online Policy