ST FRANCIS OF ASSISI CATHOLIC PRIMARY SCHOOL

E-SAFETY POLICY

Mission Statement

At St Francis of Assisi, we believe God is at the heart of our school. As a school community, we work together to provide a caring, stimulating and nurturing environment, where every child can discover their true potential and grow closer to Christ. As pupils and staff we encourage in each other a love of learning. This is a place where we can all belong and where diversity and difference is celebrated. We rejoice in each others' uniqueness and respect the dignity and beauty of each individual. Using our gifts and talents we will actively seek to make a real difference - by caring for one another and caring for our world.

1. 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 EWG 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, the 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 • 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 at this school:

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

2. Roles and Responsibilities

E-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 responsibility for e-Safety has been designated to Mrs Flack.

Our school e-Safety Co-ordinator is Mrs Vicki Flack.

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as WSGFL & Child Exploitation and Online Protection (CEOP). They take day to day responsibility for e-safety issues, provide training and advice for staff and liaises with the schools network managers (JSPC). The school's e-Safety coordinator ensures the Headteacher, senior leadership and EWG are updated as necessary.

The EWG have an overview understanding of e-Safety issues and strategies at this school. The e-safety coordinator will update the governing body at least once a year to ensure that the EWG are aware of changes in local and national guidance.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. Teachers are responsible for ensuring e-safety issues are embedded in all aspects of the curriculum and other activities.

All staff are responsible for ensuring:

- They are familiar with the schools' E-Safety policy and practices including:
  - Safe use of e-mail;
  - 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 / Cyberbullying procedures;
- Understand their role in providing e-Safety education for pupils;

- They have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP);
- They report any misuse or problem to the Headteacher/Senior Leader/e-safety Coordinator for investigation/action.

Staff are reminded / updated about e-Safety matters at least once a year.

The school includes e-safety education in both the EPR curriculum and the Computing curriculum. 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.

The school engages with parents in relation to e-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 e-safety 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.

The IT Network Manager (JSPC) is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets required e-safety technical requirements and any Local Authority E-Safety 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;
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety 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/E-safety Coordinator for investigation /action;
- that monitoring software/systems are implemented and updated as agreed in school policies.

3. Communications

How will the policy be introduced to pupils?

Many pupils are very familiar with the culture of new technologies, and have the main principles of this policy have been discussed with them. Pupils' perceptions of the risks are not always mature and hence; the e-safety rules are explained or discussed in an age appropriate manner.

E-safety education is currently placed within our SMSC Curriculum Map. We use Think U know resources to support and structure the teaching. We also integrate e-safety teaching within the curriculum map for Computing and within our Personal Goals focus annually. Each year group has a set of e-safety objectives which children are taught either in standalone computing lessons or through cross-curricula links.

How will the policy be discussed with staff?

It is important that all staff feel confident to use new technologies in teaching. Staff are given opportunities to discuss the issues and develop appropriate teaching strategies

Staff understand the rules for information systems misuse. 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.

ICT use is widespread and Induction of new staff includes a discussion of the school's e-Safety Policy.

- Staff are aware that Internet traffic is monitored and can be traced to the individual user.
- Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use are supervised by Senior Leaders and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy is provided as required.

How will parents' support be enlisted?

Internet use in pupils' homes is an everyday activity. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school is able to help parents plan appropriate supervised use of the Internet at home by:

- Encouraging a partnership approach which includes:

    - Providing parent evenings with demonstrations and suggestions for safe home Internet use;
    - Providing a designated e-safety area on our Website giving advice on filtering systems and educational and leisure activities that include responsible use of the Internet is available to parents.
    - 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 e-Safety be handled?

The school will take all reasonable precautions to ensure e-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 eSafety Coordinator / 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.

Our e-Safety Coordinator 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.

4. Managing the Internet Safely

The risks:

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a 'No Blame', supportive culture if pupils are to report abuse.

Technical and Infrastructure:
The school has a managed ICT service provided by an outside contractor (JSPC), but it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school. It is important that the managed service provider is fully aware of the school's e-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;
- Ensures their network is 'healthy' by having health checks annually on the network;
- 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;
- 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;
- 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] or only use sites accessed from managed 'safe' environments such as the Learning Platform;
- 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 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 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 - Police - the LA.

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 e-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 e-safety education programme throughout the curriculum all Key Stages, built on LA / West Sussex / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
  - to STOP and THINK before they CLICK
  - 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 on-line '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 e-safety 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;
- provision of information about national support sites for parents.

5. 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;
- 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;
- Staff use Exa network e-mail systems for professional purposes.

6. 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 eSafety education programme;

7. 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:

- 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;
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- 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; Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their USO
- 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.

9. Handling of Infringements

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

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 e-safety coordinator
- Removal of internet rights for a more extended period
- 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 e-safety 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 / EWG 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.

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).

How will staff and pupils be informed of these procedures?

- They are fully explained and included within the school's e-safety / Acceptable Use Policy. All staff will be required to sign the school's e-safety Policy acceptance form.

- Pupils are taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate e-safety / acceptable use form.

- The school's e-safety policy is made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.

- Information on reporting abuse / bullying etc. is made available by the school for pupils, staff and parents.

10. Glossary of Terms

EWG ICT MLE LA SLT WSGFL LEN s2s CTF

Executive Working Group
Information and Communication Technologies
Managed Learning Environment
Local Authority
Senior Leadership Team
West Sussex Grid for Learning
National Education Network
School to School Common Transfer File
CEOP Child Exploitation and Online Protection

May 2017