ICT E-Safety Policy

Committee Name:	Staffing
Date of Approval:	October 2015
Validity Date:	2015-2018
Person responsible:	Head Teacher

Introduction

St Fidelis, as a Rights Respecting school is committed to raising children's awareness of their rights under the UN Human Rights Charter and instil in the whole school community a sense of how these rights and values should be respected and promoted. St Fidelis is committed to practice which protects children from harm.

Staff and volunteers in this organisation accept and recognise our responsibilities to develop awareness of the issues, which cause children harm. It applies to all members of St Fidelis Catholic Primary School community (including staff, pupils, volunteers, parents / carers and visitors) who have access to and are users of school ICT systems, both in and out of St Fidelis Catholic Primary School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to pupils in the school. Teachers should ensure that the use of internet derived complies with copyright law.

Aims

We will aim to safeguard children and staff when online by:

- assisting school staff to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- setting clear expectations of behaviour and relevant to responsible use of the internet for educational, personal or recreational use.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

We are committed to reviewing our policy and good practice annually. We recognise that because of the day-to-day contact with children, school staff are well placed to observe the outward signs of abuse. The school will therefore:

- Establish and maintain an environment where children feel secure, are confident to talk, and are listened to.
- Ensure children know they can approach adults employed in the school if they are worried.
- Include opportunities in the PSHE and computing curriculum for children to develop the skills they need to recognise and stay safe from harm or abuse.

Risks

The main areas of risk for our school community can be summarised as follows:

- **Content:** exposure to inappropriate content, including online pornography and ignoring age ratings in games (exposure to violence associated with often racist language).

- **Contact**: grooming, cyber-bullying in all forms, identity theft and sharing passwords.

- **Conduct:** privacy issues, including disclosure of personal information, digital footprint and online reputation, health and well-being (amount of time spent online e.g. internet or gaming), sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images) and copyright (such as music and film).

- **Communication:** The policy will be communicated to pupils regularly through assemblies for the children and through the e-safety lessons which are placed at the start of every topic. For staff, this policy is communicated for new staff at induction and for all other staff through the Staff Handbook which is shared at regular points throughout the year. The policy is also available on the school website. Acceptable use agreements are signed by parents when children start at the school and are stored in the children's pupil file.

How will the risks be assessed?

To guard against accidental access to materials which are inappropriate we access the internet by means of the London Grid for Learning which provides an appropriately filtered service (including Google). However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT leader in order for the site to be blocked in the future.

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

- informing parents or carers;
- removal of internet or computer access for a period;

- referral to the local authority or the police.

The school's Computing Leader acts as the first point of contact for any e-safety issue. If the issue relates to staff misuse, this is handled by the Headteacher.

Should an incidence of cyberbullying arise, it will be thoroughly investigated and dealt with in accordance with our Behaviour policy. Any issue related to child protection is dealt with in accordance with the school's Safeguarding and Child Protection policy.

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on safeguarding and e-safety issues.
- Provides, as part of the induction process, all new staff including those on placement, with information and guidance on Safeguarding and Child Protection including e-safety.

Parent awareness and training

St Fidelis runs a rolling programme of advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
- Information leaflets; in school newsletters; 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.

How will ICT system security be maintained?

Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to unsuitable material. Pupils and teachers will be provided with training and regular updates in the area of Internet safety. Virus protection software will be used and updated on a regular basis. Regular back-ups are made of all school data and are kept in secure locations. The school network is regularly maintained and monitored by competent technical support.

In the Foundation Stage and Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised assess to specific, approved on-line materials.

Keeping pupils safe online
If staff or pupils discover an unsuitable site, it must be reported to the ICT leader. The Internet is for educational purposes only during school hours. Children will only be able to access the internet (at school) when under adult supervision.

Cyber-bullying is unfortunately another area which is growing rapidly. It is different from more traditional forms of bullying. Some students have 24 hour access to the internet or a mobile phone and so it can be hard to escape. The audience for the bullying can be potentially huge and comments and pictures are likely to stay online forever.

As with all forms of bullying, the School will deal with this in accordance with the Behaviour Policies (particularly the Anti-bullying and Cyberbullying policies), even if the cyber-bullying is happening outside School hours. If parents / guardians have any concerns that their child is being cyber-bullied, they should please print off any available evidence and report it to the School as soon as possible.

Helping children to safeguard themselves
Assemblies, PSHE lessons, School Trip Risk Assessments and Circle Times are a common feature of how we educate pupils to keep themselves safe at St Fidelis.

'Tell Someone' poster
The 'tell someone' poster is visible throughout the school to help children to understand that they need to speak up if they are unhappy with how someone is treating them or how someone else if being treated.

Circle Times
Circle Time is a tool used by all teachers to address issues often specific to the class involved, for example how safe children are feeling, issues relating to hygiene or resolving issues on the playground.

Learning platform

- Uploading of information on the schools' Learning Platform is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to Frog will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish Frog

Social Networking
Social networking sites (such as Facebook and Instagram) are a technology that many people– both staff and children access and enjoy using. However staff need to give due consideration to issues regarding

safeguarding and professionalism when utilising such websites. It would not be appropriate for any member of staff to have an online relationship/friendship with a pupil. If staff are contacted by a child through one of these forms of website, or feels put into any other situation that makes them feel uncomfortable, the best policy is to talk as soon as possible to one of the leadership team. Also, please think carefully about what is on your page and can be accessed by anyone – is the photograph appropriate? Is there a swear word? Do you portray yourself as a professional?

Emails

Staff are not permitted to use work emails addresses to conduct any business or communication that is not linked to the business of the school itself. Staff should maintain personal email accounts for private and personal items, and these should be kept as discrete from work related emails. Staff are asked to adjust their signature to staff emails to include the following details:

> Full Name
> Job Title
> St Fidelis Catholic Primary School
>
> *This email and any attachments to it may be confidential and intended solely for the use of the individual to whom it is addressed. Any views or opinions expressed are solely those of the author and do not necessarily represent those of St Fidelis. If you are not the intended recipient of this email, you must neither take action based upon its contents, nor copy or show it to anyone. Please contact the sender if you believe you have received this email in error.*

Personal Devices- Pupils

- St Fidelis does not allow pupils to bring mobile phones to school. Any phone found will be stored securely and parents will be contacted. It will be returned directly to the parent.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. As part of the e-safety learning, pupils are instructed in the safe and appropriate use of mobile phones and personally-owned devices and are made aware of boundaries and consequences.

Personal Devices- Staff

- As it is a legal requirement that mobile phones should not be used in the EYFS by any adults, it is sensible that their policy is applied across the school. No pupils are allowed to bring mobile phones to school. Therefore children should not see staff using mobile phones during working hours, as all staff should be focussed on the work in hand and most the importantly the children. The three exceptions are the Head Teacher, Deputy Head Teacher and Specialist PE Teacher.

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our MIS system (SIMS).

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website manager.
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. admin@st-fidelis.bexley.sch.uk. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.

Linked policies:

- ICT and Computing
- Safeguarding and Child Protection
- Anti-Bullying
- Behaviour
- Cyber Bullying

The following appendices include further information on:

- Education and Curriculum
- Expected Conduct
- Incident Management
- Internet access, security (virus protection) and filtering

Education and Curriculum

This school

- Has a clear, progressive e-safety education programme which is part of the Computing curriculum. It is built on the National Curriculum guidance. This covers a range of skills and behaviours appropriate to the child's age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- 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 how to narrow down or refine a search;
- to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable 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, location, 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;
- to understand the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted adult, or an organisation such as ChildLine or the CLICK CEOP button.
- plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

Expected conduct and incident management

Most young people experience the internet and mobile phones as a positive, productive and creative part of their activities and development of their identities. However, issues of E-Safety do arise as some students use the technologies negatively. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, evaluation and retrieval.

In this school, our children:

- are responsible for using the school ICT systems in accordance with the school's Acceptable Use policy.
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school.
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.

Staff

- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones and hand held devices.

Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for pupils to use the internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network health through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Uses security time-outs on internet access where practicable / useful;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within Frog;
- Requires staff to preview websites before use and encourages use of Frog as a key way to direct students to age / subject appropriate web sites;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , …..

- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Computing Leader. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and 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 – and the LA.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users - the London USO system;
- Uses teacher 'remote' management control tools for controlling workstations;
- Ensures the Computing leader is up-to-date with LGfL services and policies and requires the ATS to be up-to-date with LGfL services and policies;
- Storage of all data within the school will conform to the UK data protection requirements

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- All pupils have their own unique username and password which gives them access to Frog;
- We use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;

- 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;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- 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 are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by Premises Manager; equipment installed and checked by approved suppliers /engineers;
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access report writing module; SEN coordinator - SEN data;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems, e.g. RAv3 system;
- 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; e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Provides pupils and staff with access to content and resources through Frog which staff and pupils access using their username and password.
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;

- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit’s requirements;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- 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 or through USO secure file exchange (USO FX);
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Data security:
Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record in SIMS.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal.
- We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.

Technical Solutions

- Our network is managed by ATS.
- Staff have a personal, secure area on the network to store sensitive documents or photographs.
- We require staff to log-out of or lock systems when leaving their computer.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- We use RAv3 with its 2-factor authentication for remote access into our systems.

- We use the LGfL secure data transfer system, USOAutoUpdate, for creation of online user accounts for access to broadband services and the London content
- All servers are in lockable locations and managed by DBS-checked staff.
- We use LGfL's GridStore remote secure back-up for disaster recovery on our admin server.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredders.