St Mary's Catholic Primary School

FIDE ET AMORE

'With Jesus, we learn together through faith and love'

Online Safety Policy

Rationale

The Internet can offer many positive educational and social benefits to young people, but unfortunately there are associated dangers. Children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly. At St. Mary's Catholic School we value highly, the rich range of resources and experiences that the Internet, and other technologies, can offer, to both our staff and pupils.

Aims of this Policy

- To ensure that children, and staff, are working in a safe learning environment in school.
- To establish a clear understanding of the responsibilities of all those involved in the education of pupils, with regard to Internet Safety.
- To promote a safe use of the Internet by pupils at home.
- To ensure that both pupils, and staff, are aware of safe and responsible behaviours when using the Internet and E-mail.
- To teach both pupils and staff the appropriate behaviours, and critical thinking skills, to enable them to remain both safe, and legal, when using the Internet and related technologies.
- To train staff to be able to respond appropriately, and follow procedures, when dealing with issues arising from pupils' use technology.
- To ensure that the school website is effective and does not compromise the safety of pupils and staff.

Objectives:

- To ensure that an effective range of technological tools are in place to safeguard both pupils and the system itself.
- To ensure there are clear policies, and approval processes, regarding the content that can be loaded onto the school's website.
- To develop and implement a safety education programme for pupils, staff and the wider community.
- To educate pupils in acceptable behaviours when using the Internet and other related technologies e.g. mobile phones, chat rooms, games consoles and e-mail both in school and at home.
- To ensure all pupils, and staff, are aware of procedures they should follow if they come across anything that is offensive or worrying.
- To ensure all pupils are aware of sanctions that are in place if school policy is broken.
- To educate staff in acceptable behaviours when using the Internet and other related technologies when in school.
- To incorporate the teaching of appropriate Internet/E-mail behaviour.
- To encourage pupils to use their HGfL e-mail accounts, as opposed to other accounts, as this system is secure and monitored.
- To provide a scheme of work with associated activities to teach children the appropriate behaviours to enable them to remain both safe and legal when using the Internet and related technologies.
- To adopt safe practices regarding the publication of images and names of pupils on the school website.
- To ensure that the school is not infringing the intellectual property rights of others, through any publications on the school website.

Pupil Responsibilities:

Pupils must:

- Respect all equipment, hardware and software.
- Keep their email and Education City usernames and passwords safe, and secret, and are not permitted to use anyone else's usernames and passwords.
- Be aware of, and follow, the safe use of technology guidelines taught throughout the school.
- Be aware of the sanctions that are in place if these guidelines are not followed.
- Report any incidents of misuse within the school to a member of the teaching staff.
- Report any incidents of misuse outside of school to a trusted adult.
- Seek help/advice from a teacher, or trusted adult, if they experience problems when online; or if they receive any content or contact which makes them feel uncomfortable in any way.
- Communicate with their parent(s)/carer(s) about Internet Safety issues and follow school guidelines for the use of the Internet, and other related technologies, at home.
- Any accidental access to inappropriate, or banned content, must be reported to a member of school staff.
- Be aware of their social responsibilities with regard to using the Internet and other related technologies.

Pupils must not:

- E-mail malicious messages, attachments, images, or web-links to other pupils.
- Bring any form of handheld device into school e.g. mobile phones, iPads, games console etc.
- Try to access inappropriate material of any sort (including pornographic, racial hatred, religious hatred, or any material not related to the lesson).
- Pass on the usernames and passwords of others to a second party.

Please see Appendix 1 (KS1) and Appendix 2 (KS2) for our 'Pupil E-Safety Agreements'. These rules (in child-speak) are discussed in class at the start of every academic year (during our annual 'Internet Safety Week'). All pupils are asked to sign the agreements and copies are kept by the Computing Co-ordinator (Ian Morris). Poster versions of these rules are clearly displayed in each classroom and the computer suite. During our Internet Safety Week each teacher will also discuss the sanctions if a child is not following these guidelines (please see below).

Procedure:

If a pupil is found/ suspected of breaking any of the rules in the 'Pupil Internet Safety Agreement' the Computing Co-ordinator should be informed. Sanctions will be discussed and imposed, in accordance with Appendix 3. All incidents are recorded in the 'Internet Safety Log Book'.

Acceptable use of E-Technolgies by Staff

It is important that when members of school staff communicate with pupils they remember their professional role.

Communication between children and young people, by whatever method, should take place within clear and professional boundaries. This includes the wider use of technology such as mobile phones, text messages, emails, digital cameras, web-cams, websites and blogs.

This means that staff should:

- Not give their personal contact details to pupils, including their mobile telephone number, or personal email address.
- Not use the internet or web-based communication channels to send personal messages to pupils.
- Be aware of information that they are putting into the public domain (Facebook, Twitter etc.) Do not allow children or young people to be listed as their "friends" and do not allow themselves to be listed as "friend" on their sites.
- Not request or respond to any personal information from a pupil.
- It is the legal responsibility of ALL members of staff to adhere to the school Child Protection Policy and to report any concerns to the school Child Protection lead (Miss Shevlin).

Email or text communication between a member of staff and a pupil may lead to disciplinary and/or criminal investigations. This also includes communications made through internet sites.

Social Media

Discussing school or making reference to any child, staff member or groups of children is very unprofessional and against safeguarding and confidentiality practices.
No member of staff should ever allow a child or ex-pupil to become a friend on Facebook. This is a serious Safeguarding issue.
Staff need to ensure their security settings are fixed carefully on Facebook as lack of tight security could lead to parents or children knowing about your personal life compromising your professionalism of working in a school.
Staff should not access Facebook during their working hours (For example on a mobile phone). Mobile phones should never be used in classroom or playground in front of children.
I understand that the above actions could lead to disciplinary action and will compromise my position as a professional working in school.

Staff Responsibilities:

Mobile phones must not be used to record images/videos of pupils (eg. on school trips). School cameras may be used to record images of pupils, but these must be downloaded onto the school computer network and removed from the device at the end of the day. School staff have a right to access these files for educational purposes only.

All members of staff have individual responsibilities to protect the security and confidentiality of the school computer network. Passwords must not be shared and **ALL staff must log off the teacher desktop** when they leave a machine unattended. The Internet and e-mail may be used in school for educational purposes. It **should not be used for personal purposes** such as booking holidays, or viewing entertainment media. Staff must take measures to protect the system against viruses. **They must use a virus checker when using removable media such as USB Pen-drives**.

The Internet and related technologies are not to be used for any form of illegal activity, for example downloading copyright materials, or accessing banned content.

The use of the Internet and e-mails are monitored by the HGfL. E-mails and Internet searches are also filtered through LA systems. Firewalls and anti virus protection is in place and covers the one feed from the LGfL to the World Wide Web. **Accidental access to inappropriate or banned content must be reported** to the Computing Co-ordinator. They will make a note in the 'Internet Safety Log Book' and provide the borough with the URL to be blocked.

Staff should not take home any Lap-top, iPad or other device without first consulting the Head Teacher. If permission is given a note should be made in the 'Equipment Sign-Out Book' kept in the front office. **School laptops/iPads must not be used for any illegal or inappropriate activities e.g. access to, or sharing of banned content.**

Procedure:

Reported incidents of staff misuse should be reported to the head Teacher, Computing Co-ordinator and appropriate staff at the LA. Outside agencies, including the police and counselling services, will be informed if deemed appropriate. All incidents will be logged in the 'Internet Safety Log Book'. Legal advice will be obtained in cases of suspected illegal activity.

Any evidence of illegal behaviour on a school computer, laptop or other related technology will result in the isolation of the machine and maybe the freezing of the network. The police will be informed and the Head Teacher is to seek legal advice from the borough as soon as possible.

Accidental access to inappropriate or banned content must be passed to the Borough for blocking.

Policy for the use of e-mail in school

Staff are encouraged to share information through use of e-mail and it provides pupils with learning experiences that conventionally, would not be possible. We aim to continue developing the role of e-mail within the school but we need to be aware of harmful behaviours and how to deal with them (examples may include bullying, viruses, spamming and malicious attachments.)

Responsibilities

HGfL:

- To install and maintain e-mail filtering and monitoring software.
- To provide anti-virus software and keep it up to date.
- To provide e-mail addresses, usernames and passwords for all staff and pupils. Pupil usernames are randomly selected, preventing people working out which account belongs to whom.

School Staff:

- To inform the Computing Co-ordinator if a pupil informs them of any misuse of e-mail.
- To teach responsible behaviours when using e-mail.

School Pupil:

- To inform their teacher if they receive a malicious message, or an unknown attachment.

- To keep their HGfL username and password safe and not to use the usernames and passwords of others for any reason.
- To not send malicious, bullying or inappropriate material of any kind in any form - image, text, video, web link or attachment.
-

Procedures:

If a pupil is found/ suspected of sending nasty E-mail messages/attachments or mis-using their own/ or another child's account then the Computing Co-ordinator should be informed. Sanctions will be discussed and imposed, in accordance with Appendix 3. The Computing Co-ordinator will record all incidents in the 'Internet Safety Log Book'.

Policy for the teaching of Internet Safety

Every year, we hold our annual Internet Safety Week in school. All teachers reinforce the school rules for using the computers, the Internet and E-mail in school. All pupils sign the 'Internet Safety Agreements; (Appendix 1 and 2) agreeing to follow the school rules as appropriate in each Key Stage. Cross-curricular work is covered, related to Internet Safety, and it is the focus for the computing lesson for this week.

A copy of the KS1 and KS2 Internet Safety Rules are clearly displayed in each classroom. The school follows the 'Switched on Computing' scheme of work. Internet Safety opportunities are identified across all of the topics taught each half term

School Website

Responsibilities and procedures:

Access to website administration (via password) is strictly restricted to named members of the administration team and the Senior Management Team. These named individuals have been trained for the uploading and maintaining of current information. The SMT will approve the content to be uploaded onto the website and will monitor what is on the site on a half termly basis. Any content deemed inappropriate will be removed and its source investigated.

The copyright of any content uploaded to the site is checked and if necessary, indicated on the site. If any reports of images being used inappropriately reach the school, the Head Teacher, Deputy Head Teacher and E-Safety Co-ordinator will be informed if deemed necessary. Legal advice will be sought from the LA if deemed necessary and the police will be informed.

Appendix 1

KS1 Pupil Internet Safety Rules

- Take care of all the computers and headphones in school.
- Do not send any nasty messages when using the computers.
- Do not tell people your name, address, telephone number, or school when using the Internet.
- Keep your computer passwords a secret.
- Do not use a password for somebody else in your class.
- Only use the computers in school when you are with an adult.

I will follow these rules when using the computers in school and at home.

My Name: ____________________ Year: ___

Date: __________

Appendix 2

KS2 Pupil Internet Rules

- Take care of all ICT equipment.
- Keep your computer passwords a secret (do not use another child’s password).
- Do not bring Pen-drives, mobile phones or hand-held games consoles into school.
- Only E-mail people you know (or somebody your teachers/parents have approved).
- Do not share your name, address, phone number, or school with people you meet on-line.
- Don’t send anyone photographs of yourself, friends or family without first talking to a trusted adult.
- You are not allowed access to Chat Rooms, private E-mail accounts or social media sites in school. Talk to your parents before joining one at home. You should not be a member of ‘Facebook’ (as users should legally be 13 years old to sign up).
- Never agree to meet an online friend in real life without checking with your parents.
- Do not send any kind of nasty message on-line.
- Only use the computers and Internet in school when you are with an adult (only search for topics they have asked you to).
- Tell a trusted adult if you see something on the Internet/E-mail that upsets you (e.g. a nasty message).

Use of the Internet and E-mail.

I understand the rules I must follow when using computers, the Internet and E-mail.

My Name: ______________________   Year: ___

Date: ___________

Appendix 3

Staff Internet Safety Agreement

Staff should:

- Not give their personal contact details to pupils (excluding family members).
- Not use the Internet, or social media, to send personal messages to pupils (excluding family members).
- Mobile phones must not be used to record images of pupils. School cameras may be used to record images, but these must be downloaded to the school computer network and not taken home. All staff have the right to access these files for educational purposes only.
- Colleagues must keep their Hgfl and School Network usernames, and passwords, a secret.
- Staff should not use the usernames and passwords of any other adult working in school.
- It is the responsibility of all staff to **'log off' from the 'Staff' log-in** and Target Tracker screen after using a PC. These folders contain private, sensitive information that should not be freely visible to pupils and other adults.
- The Internet should **only** be used in school for **educational/ school purposes**. It should not be used for personal purposes such as viewing entertainment media or viewing/ booking holidays.
- Staff must take measures to protect our computer network against viruses and should only use removable media (such as a pen-drive) after carrying out a virus check.
- The Internet, and related technologies, are not to be used for any form of illegal activity e.g. downloading copyright materials, or accessing banned content.
- Accidental access to inappropriate, or banned content **(including pornographic, racial hatred or religious hatred web-sites)**, must be reported to the E-Safety Co-ordinator. They will record the incident in the 'E-Safety Log-Book' and report the URL to the Hgfl for blocking.
- Staff should not take home any Lap-top, iPad, school equipment, or confidential data without first consulting with the Head Teacher. If permission is given, a written record should be made in the 'Equipment Sign-Out Book' (kept in the front office). **School laptops must not be used for any illegal or inappropriate activities e.g. access to, or sharing of banned content.**
- Staff have the responsibility of passing any Internet Safety concerns to a member of the SMT.

<u>Social Media Sites and other Internet Communication</u>

On Facebook, or other internet communication, discussing school or making reference to any child, staff member or groups of children is very unprofessional and against safeguarding and confidentiality practices.

No member of staff should ever allow a child or ex pupil to become a friend on Facebook (excluding family members or adults over the age of 18). **This is a serious Safeguarding issue.**

Staff should ensure their security settings are fixed carefully on Facebook as a lack of tight security could lead to parents, or children, knowing about your personal life and compromising your professionalism of working in a school.

Staff should not access Facebook during their working hours (For example on a mobile phone). Mobile phones should never be used in a classroom, or in one of the playgrounds, in front of children.

I understand that the above actions could lead to disciplinary action and will compromise my position as a professional working in school.

I have read and shall comply with the above Safeguarding and Heath and Safety matters. I understand that all members of staff have a responsibility for Safeguarding and Health and safety in the school.

Signed: _________________________ **Date: ___________**

Print Name: ______________________________

Appendix 4

<u>Pupil sanctions for misuse of the Internet and other related technologies</u>

Misuse	Procedure	Sanction
ICT equipment not treated with respect e.g. damage or deletion of files.	Class teacher to discuss issue with child and impose appropriate sanctions in accordance with the Behaviour Policy. Parents to be informed. Offence to be logged by the E-Safety Co-ordinator in the 'E-Safety Log Book'.	Parents informed.
Deliberate access of another person's e-mail account.	If a pupil is found to be using usernames and passwords (other than their own) then the E-Safety Co-ordinator is to be informed who will consult with the head teacher. Sanctions appropriate to the offence will be discussed and implemented. Offence to be logged.	Parents informed. Warning. Re-occurrence will lead to a two week 'freezing' of the perpetrators accounts. Further re-occurrence could lead to permanent 'freezing' of perpetrators accounts.
Passing on the account usernames and passwords of others to a second party	If a pupil passes on the account usernames and passwords of others to a second party then the E-Safety Co-ordinator and the head teacher are to be informed. Offence to be logged.	Parents informed. Warning. Re-occurrence will lead to a two week 'freezing' of the perpetrators accounts. Further re-occurrence could lead to permanent 'freezing' of perpetrators accounts.
Trying to access chat rooms or social media sites	If a pupil tries to access chat rooms or Instant Messaging Services then the E-Safety Co-ordinator and the head teacher are to be informed. Offence to be logged.	Parents informed.
Sending malicious messages using communication technology	If a child is found to be sending offensive or malicious messages via e-mail or other communication technologies then the E-Safety Co-ordinator is to be informed who will consult with the head teacher. Sanctions appropriate to the offence will be discussed and implemented. Offence to be logged.	Parents informed. Warning. Re-occurrence will lead to a two week 'freezing' of the perpetrators accounts. Further re-occurrence could lead to permanent 'freezing' of perpetrators accounts.
Knowingly sending malicious e-mail attachments	If a child is found to be malicious attachments via e-mail or other communication	Parents informed. Warning. Re-occurrence will lead to a two week 'freezing' of the

	technologies then the E-Safety Co-ordinator is to be informed who will consult with the head teacher. Offence to be logged.	perpetrators accounts. Further re-occurrence could lead to permanent ‘freezing’ of perpetrators accounts.
Bringing mobile phones or other prohibited handheld devices into school	Confiscation, inform parents. Hand back to parents. Offence to be logged.	Parents informed
Deliberately trying to access inappropriate or banned content	If a child is found to be trying to deliberately access inappropriate material (pornographic sites, racial hatred or religious hatred, sexist jokes, drug or bomb making recipes) then their class teacher, head teacher and parents to be informed, issue discussed. Procedures outlined in Behaviour Policy to be followed. Outside agencies should be alerted if deemed appropriate by the Head Teacher.	Parents informed. Warning. Possible suspension for repeat offence.
Sending messages via communication technology relating to racial or religious hatred	Any messages of bullying related to Racial Hatred or Religious Hatred to be reported to the E-Safety Co-ordinator and Head Teacher and the police informed if deemed necessary. Legal advice to be taken from the LEA, parents consulted and incident logged. Appropriate sanctions implemented. Counselling may need to be offered to both victim(s) and perpetrator(s).	Parents informed. Warning. No unsupervised access to school computer equipment. Possible suspension for repeat offence.
Using communication technology for the purpose of bullying others.	Follow guidelines in Anti-Bullying Policy	Parents informed. No unsupervised access to school computer equipment. Follow guidelines in Anti-Bullying Policy