Saint John Fisher Catholic Primary School

ICT E-Safety Policy

"To live, love and learn and learn in our caring community."

Saint John Fisher Catholic Primary School

ICT E-Safety Policy

Content

Introduction

National guidance suggests that it is essential for schools to take a leading role in e-safety.

Becta in its "Safeguarding Children in a Digital World" suggested:

> *"That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too."*

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

> *"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."*

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to learners. The benefits are perceived to "outweigh the risks." However, schools must, through their e-safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. This e-safety policy also forms part of the school's protection from legal challenge, relating to the use of ICT.

Background/Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy helps to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Principal and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, it can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with behaviour/ anti-bullying/ child protection policies.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

This e-safety policy explains how we intend to demonstrate that we provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks, whilst also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Schedule for Development/Monitoring/Review

This e-safety policy was approved by the *Governors on:*	Date:
The implementation of this e-safety policy will be monitored by the:	Principal, ICT Co-Ordinator and the Senior Leadership Team
Monitoring will take place at regular intervals:	Annually
The *Governors Sub Committee* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually
The E-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 e-safety or incidents that have taken place. The next anticipated review date will be:	July 2013

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of
  - pupils (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)
  - parents / carers
  - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. This policy applies directly to the school curriculum network and not the administration network. The administration network is not currently accessible by most staff and the main responsibility for this lies with the Principal whilst the main responsibility for the curriculum network lies with the ICT Co-Ordinator.

The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of *E-Safety Governor*. The role of the E-Safety Governor will include:

- meetings with the Principal and / or ICT Co-ordinator
- monitoring of e-safety incident logs
- reporting to relevant Governors meeting

Principal and Senior Leaders:

- The Principal is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the ICT Co-ordinator.
- The Principal / Senior Leaders are responsible for ensuring that the ICT Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Principal / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Principal and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

ICT Coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting of Governors
- reports to Senior Leadership Team

- is responsible for ensuring that users may only access the school's networks through a properly enforced password protection policy
- is responsible for ensuring that she keeps up to date with e-safety technical information in order to effectively carry out the e-safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies
- provides education / information for parents / carers regarding e-safety for their children

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the ICT Co-ordinator for investigation
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) are on a professional level
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that any unsuitable material that is found in internet searches is reported to the ICT Co-Ordinator

Designated person for child protection

should be trained in e-safety issues and be aware of the potential for serious child protection 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
- cyber-bullying

These are child protection issues, not technical issues, and as such are covered by the Child Protection Policy. The technology simply provides additional means for child protection issues to develop and the child protection officer and ICT Co-Ordinator responsible for e-Safety should work closely together.

Pupils

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. In KS1 it is expected that parents / carers will sign on behalf of the pupils.
- will be taught to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations and they will respect this
- 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 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.
- 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

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing the school website / VLE / on-line pupil records in accordance with school policy.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Rules for use of ICT systems / internet will be displayed
- Staff will act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).
The school will, therefore, seek to provide information and awareness to parents and carers through

- Letters, newsletters, VLE
- Parents evenings

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff with network access should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- A planned programme of formal e-safety training will be made available to staff.

- The ICT Coordinator will receive regular updates from the LA and will be able attend training sessions and review guidance documents as appropriate.
- This E-Safety policy will be presented to and discussed by staff in staff meetings / INSET days.
- The ICT Coordinator or members of the Senior leadership Team will provide advice / guidance / training as required to individuals as required

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password for both the school network and the Virtual Learning Environment by the ICT Co-Ordinator. Users will be required to change their password for the Virtual Learning Environment.
- The administrator password for the school ICT system, used by the ICT Co-Ordinator must also be available to the Principal or other nominated senior leader, but will not be made available to other staff unless there is a specific and significant need.
- The school has historically provided enhanced user-level filtering through the use of the Resdstone filtering programme provided through the LA, this is likely to change in the near future to enable the school to have more control over the filtering. Enhanced user-level filtering will, however, remain in place and be managed by the ICT Co-Ordinator.
- When the filtering is managed in-house - in the event of needing to switch off the filtering for any reason, or for any user, this must be logged and carried with the agreement of the Principal or ICT Co-ordinator.
- When the filtering is managed in-house - requests from staff for sites to be removed from the filtered list will be considered by the ICT Co-Ordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Principal.
- The ICT co-ordinator can monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Downloading of executable files by users is only allowed with the permission of the ICT Co-Ordinator or Principal.
- School laptops and other portable devices should not be used for personal use of staff or pupils. No family members are allowed on laptops and other portable devices that may be used out of school. (see School Personal Data Policy for further detail)

- Staff are forbidden from installing programmes on school workstations / portable devices without written permission from the ICT Co-Ordinator or Principal.
- An agreed policy is in regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices. (see School Personal Data Policy for further detail)
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.(see School Personal Data Policy for further detail)

Curriculum

E-safety should be a focus in all areas of the curriculum and all staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that 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.
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Co-Ordinator or Principal temporarily removes those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught by all staff in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.

- Staff will not publish any digital images of themselves or other staff engaged in school activities on the personal pages of social networking sites, unless they have obtained written permission from the Principal to do so.
- Staff will not publish any digital images of pupils engaged in school activities on their personal pages of social networking sites.
- Staff will ensure that their personal networking use is restricted so that it is not publicly available and will ensure that at all times their use related to the school remains professional and does not bring the school into disrepute. This includes, but is not exclusive to, ensuring that pupils of the school do not have access to their personal sites unless there are good personal reasons.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs of pupils / pupils are published on the school website- this permission will be covered as part of the AUP signed by parents or carers at the start of the year. This will be done on the basis that parents/ carers must write explicitly to say if they do not want their child's image to be used in this way.

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.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. A School Personal Data policy which our school has adopted is available in the appendices to this document.

Staff must ensure that:

• At all times they take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

• they change their school password so that it is not known by pupils.

• they use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of every use.

• they transfer data using securely.

• they do not store personal data on any portable USB stick or any removable media:

• Personal data stored on laptops must either be encrypted and password protected or must only be available for access by the registered user via a secure logon or the administrator. The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

• they do not use personal email addresses on school equipment or for school purposes.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x							x
Use of mobile phones in lessons		x						x
Use of mobile phones in social time	x							x
Taking photos on mobile phones or other camera devices		x						x
Use of hand held devices eg PDAs, PSPs	x				x			
Use of personal email addresses in school, or on school network				x				x
Use of school email for personal emails				x				x
Use of chat rooms / facilities		x					x	
Use of instant messaging		x					x	
Use of social networking sites in school other than VLE				x				x

Use of blogs	x				x			

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff should therefore use only the school email service to communicate with others regarding school business. Pupils should use only the school email service to communicate with others when in school, or on school systems.
- Users need to be aware that email communications may be monitored.
- Users must immediately report – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils / or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material. This will form part of the ICT curriculum but must also be reinforced by all staff.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities eg Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					×
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					×
	adult material that potentially breaches the Obscene Publications Act in the UK					×
	criminally racist material in UK					×
	pornography				×	
	promotion of any kind of discrimination				×	
	promotion of racial or religious hatred				×	
	threatening behaviour, including promotion of physical violence or mental harm				×	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				×	
Using school systems to run a private business					×	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				×		
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions						×
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					×	