St Mary's P.S.

TOGETHER FOR CHILDREN

E- SAFETY POLICY

November 2015

Introduction

The purpose of this policy is to ensure all pupils, staff, parents and governors understand and agree the school's approach to e-safety. This policy should be read, understood and applied in conjunction with the school's policies for Child Protection (including Anti-Bullying, Positive Behaviour, Acceptable Use of the Internet).

This policy applies to all who have access to the school's ICT systems and equipment, both in and out of school.

Teaching and Learning

The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the management information and business administration systems. Access to the Internet is a necessary tool for staff and students and is a requirement within the NI Curriculum. It helps pupils prepare for their continued personal development.

Internet access within St Mary's is provided by c2kni and is designed to be safe for all users. This includes each individual having their own log-in and password, as well as filtering content appropriate to the age of pupils. Access to the Internet is planned to enrich and extend learning and is reviewed to reflect the appropriate curriculum requirements.

When age-appropriate, pupils are

- Given clear guidance on safe use of the Internet, are taught how to take responsibility for their own Internet access and sign an Internet Use Agreement
- Are taught ways to validate information before accepting it is necessarily accurate
- Are made aware the writer of an e-mail or the author of a web page might not be the person claimed
- Are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable

Managing Internet Access

Our school computer network is managed by c2kni to ensure it is safe and appropriate for pupils.

E-Mail (Pupils)

- As yet pupils do not have access to school-based e-mail accounts but they are made aware that
- They must be very vigilant about using e-mails as a means of communication
- They must tell a teacher immediately if they receive offensive e-mail
- They must not reveal their personal details, those of others or arrange to meet anyone without specific permission from their parents
- They should not open suspicious incoming e-mail or attachments

E-Mail (Staff)

C2k recommend all staff should be encouraged to use their c2kn e-mail system. It is strongly advised staff should not use home e-mail accounts for school business. The c2k Education Network filtering solution provides security and protection to c2k e-mail accounts. The filtering solution offers scanning of all school e-mail ensuring both incoming and outgoing messages are checked for viruses, spam and inappropriate content.

Social Networking

Pupils will not have access to sites such as Facebook but we are very aware social networking plays a huge part in children's online activity. We realise many of our pupils will have access to Facebook accounts at home and we therefore aim to build their awareness as too how to use these sites appropriately. Pupils will be informed

- To keep personal safety when using such sites
- Not to get involved in cyber-bullying
- That parents will be informed immediately of any breaches either during or after school

Pupils may, from time to time, use chat rooms within the c2kni network as part of supervised class ICT activity but only when using the filtered network within school and only when supervised by an adult.

Cyber Bullying

School is aware pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying is also considered within St Mary's Anti-Bullying Policy.

Cyber bullying can take many different forms including:

- E-mail – nasty or abusive e-mails which may include viruses or inappropriate content
- Instant Messaging (IM) or chat rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile
- Online Gaming – abuse or harassment of someone using multi-player gaming sites
- Mobile phones – examples can include abusive texts, video of photo messages
- Abusing personal information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded all incidents of cyber-bullying will be treated within the school's anti-bullying policy.

Use of Images on School Web Site

Our school website compiles with the school's guidelines for using images.

Eg

- Photographs used will not identify individual pupils
- Children's photographs are only used once written permission has been received from the child's parent/carer
- Children's photos are not accompanied by names
- Children's work which contains photographs must also not contain the child's name

Filtering of Content

The school works in partnership with parents, DENI, EA and c2kni to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, they are informed the URL (address) and content must be reported to the ICT Co-ordinator who will then inform c2k.

Managing Video Conferencing

Video conferencing is used in upper KS2 classes and uses only the approved program. Pupils are made aware of the need to behave appropriately and are always supervised by an adult.

Access to video conferencing is always appropriately planned and managed by members of staff. Pupils have no independent access to webcams etc.

Managing Mobile Phone Technologies

- Mobile phones must not be used for photographing pupils
- Smartphones are not to be used within the school day for accessing the Internet
- Only school cameras are used by both staff and children for educational purposes

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Staff must not keep confidential information on removable devices such as USB devices unless suitably security protected.

Policy Decisions

Authorising Internet Access

The school maintains a record of all staff and children who have access to the school's ICT systems.

Parents and children are asked to sign a consent form regarding their child's internet use.

Assessing Risks

The school takes all reasonable precautions to prevent access to inappropriate material. 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 computer connected to the school network. The school will endeavour to ensure that inappropriate content is not accessed but cannot accept liability if any such material evades our filtering systems. The school's E-Safety policy and its implementation will be monitored and reviewed on a regular basis.

- As part of their learning, children will be made aware, as appropriate, of the needs to protect themselves from harmful material while online. This will be done on an age-appropriate basis.
- Pupils will know they are to inform an adult if any inappropriate material becomes evident during the school day.

Handling E-Safety Complaints

- Complaints of pupil/staff Internet misuse must be referred to the Principal
- Complaints of a child protection nature will be dealt with in accordance with the school's Child Protection Policy
- Pupils and parents are informed of the Complaints Procedure
- Pupils and parents are informed of the consequences for pupil misuse if the Internet

Communications Policy

Introducing the E-Safety Policy to Pupils

- E-Safety Posters are displayed
- Pupils are informed that network and Internet use is monitored and appropriately followed up
- Children receive E-Safety lessons and are constantly reminded of online safety

Staff and the E-Safety Policy

All staff are trained to monitor children's Internet use and receive a copy of the policy. Staff are informed that network and Internet traffic can be traced to an individual user.

Enlisting Parents'/Carers' Support

Parents' and carers' attention is drawn to the school's E-Safety Policy in Newsletters and on the school website. The school has links on its website to E-Safety resources. Parents are asked to sign the agreement for Internet use.

Roles and Responsibilities:

Governors:

- Policy adoption
- Representation on the e-safety committee
- Discuss e-safety at meetings
- Monitor the e-safety log

Principal and Senior Leadership Group

- Principal has a duty of care for ensuring the safety of members of the school community.
- Safeguarding Team members should all be aware of procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Officer

- Leads the e-safety team
- Takes day to day responsibility.
- Manages the review of the policy.

- Ensure staff are aware of procedures in the event of an incident.
- Provides training for staff
- Liaises with relevant external bodies.
- Maintains a log of incidents.

Network Manager

- Ensures the ICT system is secure and not open to misuse
- Liaises with c2k
- Ensures that users may only access the network and devices through a properly enforced password protection policy in which passwords are regularly changed.
- Keep abreast of current developments.

Teachers and Learning Support staff

- Have an up to date awareness of e-safety policy and practice
- Have read, understood and signed the Acceptable Use Policy.
- Report suspected misuse to the Principal
- Maintain all digital communications with pupils, parents and colleagues on a professional level.
  E-Safety Team:
- Review and monitor the e-safety policy.
- Monitor the incident log.
- Consult stakeholders on e-safety provision.
- Use the 360 degree self-evaluation tool

Pupils

- Be responsible for using the digital technology systems in accordance with the Acceptable Use Policy.

Parents

- Support the school in ensuring good e-safety practice.
- Follow guidelines in associated policies for Use of Mobiles, use of digital images taken at assemblies, sporting and other events.

Policy Statement

Education of Pupils

E-safety should be a focus in all areas of the curriculum and staff should re-enforce e-safety messages cross the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned digital literacy and e-safety curriculum which is integrated into RE, PDMU, ICT, and Literacy.
- Key e-safety messages should be re-enforced as part of the planned programme of assemblies, after school clubs or inter-school projects.
- Pupils should be taught to be critically aware of 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.

Education of Parents

The school will seek to provide information and awareness to parents through:

- Newsletter messages
- Assemblies
- Information sessions
- Website links
- Safer Internet day

Education of Staff

- A planned programme of formal e-safety training should be made available to staff. The programme should be updated and re-enforced regularly.
- An audit of training needs should be carried out.
- New staff should receive e-safety training / information as part of their induction so that they fully understand the e-safety policy and Acceptable Use agreements.

Education of Governors

- Governors should take part in e-safety training/ awareness sessions whether provided by NEELB or the school.

Technical Infrastructure

- This is managed by c2k and the school complies with guidance provided.
- Servers are located away from pupils.
- All users have clearly defined rights as agreed with the c2k manager
- All users are provided with a username and password.
- The administrator password used by the c2k manager should be made available to the Principal and kept in a secure place.
- Internet access is filtered for all users.

Bring Your Own Device (BYOD)

- Currently the school does not permit pupils to bring their own device so as not to introduce vulnerability to our e-safety considerations.

Digital Images

- Staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images and in particular their own images on the internet.
- Images of pupils should always be stored centrally and removed from any device taken outside the school premises.

Data Protection

The school ensures that…

- We hold only the minimum data required for the minimum time required and in keeping with the Disposal of Records Schedule (EA)
- Inaccuracies will be corrected without unnecessary delay.
- We have a Data Protection Policy
- We are registered with the Information Commissioner and Data Controller.
- Staff keep safe, all personal data belonging to pupils to minimise risk of loss or misuse
- Use personal data on only secure password protected computers and other devices

Communications

- The c2k email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must report immediately, any communication which makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff/ pupils / parents must be professional in tone and content.

Social Media Protecting Professional Identity

- The school has a duty of care to provide a safe learning environment for pupils and staff and could be held responsible, indirectly for acts of employees in the course of their employment. Staff who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
- Training includes acceptable use, social media risks, checking of settings, data protection, reporting issues.
- Risk assessment is carried out.
- Staff should ensure no reference is made in social media, to pupils, parents, or school staff.
- Staff should not engage in on-line discussion on personal matters relating to the school community.
- Staff should ensure that personal opinions should not be attributed to the school.
- Staff should ensure that security settings on personal social media profiles are regularly checked to reduce the risk of loss of personal information.
- If the school uses social media for professional purposes, this will be checked regularly by the e-safety team to ensure compliance with all policies

Responding to Instances of Misuse

It is hoped that members of the school will be responsible users of digital technologies. However there may be times when infringements could occur either through carelessness, irresponsible use or very rarely, through misuse. SEE THE FLOWCHART.

If monitoring reveals images of Child Abuse then the monitoring should be halted and the Police should be referred to immediately. The same applies to:

- Incidents of 'grooming' behaviour
- Sending obscene images to a child
- Adult material
- Criminally racist material
- Other criminal conduct.

In such instances, the computer should be isolated immediately. Any change to its state may hamper police investigation.

This document results from detailed guidance from SWGfL.

Responding to incidents of misuse – flow chart