**St. John’s P.S.**



**E- SAFETY POLICY**

**November 2014**

**Reviewed / updated / adopted October 2015/ March 2017/ January 2020/ February 2023**

**Originally Devised by the e-safety Group (Principal-Mrs Kearney, ICT Co-ordinator-Mr McEldowney, e-Safety Governor-Mr David Reid) and in consultation with staff, Governors, parents and pupils.**

**School Awards:**

* **Digital School of Distinction**
* **Cyber Resilience and Internet safety**

Scope of Policy: Applies to all who have access to the school’s ICT systems and equipment, both in and out of school.

Links to other Policies: 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, Use of Mobile Phones.

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/ checks Securus reports on c2k

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 the EA 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 (Mr McEldowney)
* 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.
* Staff leaving employment at St. John’s should ensure that any images are removed from any storage system they possess and remain in the school.

**DATA PROTECTION**

The school ensures that…

* We are compliant with GDPR guidelines and policies.
* 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 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.
* Staff relinquish any data held and ensure it remains in the school.
* Use of the Gsuite opt-in service via c2k single sign-on means cloud storage is in use but is governed the same as school-based storage.

**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 INCIDENTS 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 BELOW

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

