ST BRIGID'S PRIMARY, NURSERY SCHOOL AND AUTISTIC CENTRE.

E-Safety Policy

Policy Reviewed Spring 2017

Next Review Date Spring 2018

Signed …….. Chair of Governors
Signed…….. Principal

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 for everyone. The 'MySchool' and 'Fronter' services present many opportunities for all pupils. It will give teachers and pupils access to learning resources from across the world and will bring these resources into the classroom. Access to the 'digital classroom' and its e-learning tools, lessons and resources will be possible from any internet connected device, 24 hours a day. This allows teachers, pupils and parents to work in partnership to support learning. Children and young people have an entitlement to safe internet access at all times. Therefore, the guiding principles from the D.O.E Online Safety Circular No:2016/17 will be integrated into our preventative education curriculum to enhance online safety at St Brigid's

This e-safety policy links with other Pastoral care policies. It is integrated into existing safeguarding/child protection, behaviour, code of practice and anti-bullying policies. This policy has has been developed by the teaching staff of St Brigid's with the UICT Co-ordinator. Consultation with the whole school community has taken place through the following:

- Staff meetings
- School / Student / Pupil Council/ assemblies
- Governors meeting / sub committee meeting
- Letters to parents

Roles and Responsibilities

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 / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. The role of the e-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator / Officer
- regular monitoring of e-safety incident logs
- reporting to relevant Governors committee / meeting

Principal and Senior Leaders:

- The Principal and Governors are 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 e-Safety Co-ordinator.
- The Principal / Senior Leaders are responsible for ensuring that the E-Safety 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 one member of the Senior Leadership Team / Senior Management Team will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed and monitored by C2k.

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 will monitor pupil use on an ongoing basis and report any suspected misuse or problem to the E-Safety/UICT Co-ordinator or Principal for investigation.
- digital communications with pupils (email / Virtual Learning Environment (VLE) or voice) are on a professional level
- They deliver an age related on-line safety curriculum to enable children to become safe and responsible users of technology.

Designated person for child protection / Deputy designated Child Protection Officer
will 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

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. The school will help parents to understand these complex issues. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy.

Pupils :

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign along with their parents before being given access to school systems.

Education – Our school will take preventative action and deliver preventative education to protect children and minimise the associated risks around online safety. It is acknowledged that these new technologies can put young people at risk within and outside the school. These risks have been defined under four categories according to D.O.E circular 2016/7.

- CONTENT RISKS: The child is exposed to harmful materials such as inappropriate images, unsuitable video/ internet games .
- CONTACT RISKS : The child participates in adult-initiated online activity and/or is at risk of grooming. Inappropriate communication / contact with others, including strangers

- CONDUCT RISKS: The child is a perpetrator or subject to bullying behaviour (cyber bullying) in peer to peer exchange and/or at risk of bullying, entrapment or blackmail. The sharing / distribution of personal images and information without an individual's consent or knowledge

- COMMERCIAL RISKS: The child or young person is exposed to inappropriate advertising, marketing schemes or hidden costs/fraud.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum. Pupils will be guided to suitable sites by their teacher. E-Safety education will be provided in the following ways:

- A planned whole school e-safety programme provided as part of PDMU/UICT lessons , assemblies, School Council meetings. This will cover both the safe use of ICT and new technologies in school and outside school. Pupils should now follow the five golden rules for being smart and safe online(Childnet guidance 2017) Pupils will participate in Safer Internet day activities and associated competitions.The pupils will also have a planned progressive online safety curriculum for each year group.

The school may from time to time provide information and training for parents.

Education & Training – Staff

All staff will be kept up to date with e- safety policy training and developments.

- It is agreed that all staff- teachers, sub teachers, students and guests will use the ICT systems in a professional and responsible way.

Use of digital Images - Photographic, Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, using, sharing, publishing 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.

- Video and digital images are only to be used with the person's permission. School iPads are to be used for educational purposes only. *Mobile phone use by pupils is not allowed in school and they must be handed into the office if found onsite.*

Data Protection

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

Communications/ Social Media

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 by C2K. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications will be monitored
- Users must report immediately to nominated person, the receipt of any e-mail that makes them feel uncomfortable or is offensive, threatening or bullying in nature. They must not respond to any such email.

- Any digital communication between staff and pupils or parents (email, chat, VLE etc) must be professional in tone and content.
- While the school may use social media accounts to communicate with parents, no social media platforms will be used with primary school pupils.

Monitoring and Evaluation

The school will keep an up to date record of potential breaches of online Safety in an Online Safety Risk Register. Our school policy restricts certain internet usage as follows:

Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material relating to inappropriate activities.

Our school will apply the C2K filtering system as appropriate with no children allowed access to internet streaming including You Tube or social networking. Pupils have limited access to google searches and this is filtered by C2k.

The principal or SLT may request an internet usage report on an individual if needed. Securus may be used in future to monitor pupil internet usage if it is deemed necessary.

Responding to incidents of misuse

If any misuse is observed, it should be reported to a teacher by a pupil or to principal/vice principal by a teacher. The principal may wish to inform the Governors or other related outside agencies- social services, Welb, Police.

In cases of pupil misuse, pupils will have internet access removed for a specified period of time. Other sanctions may apply depending on the incident.