Online Safety Policy

St Bride's Primary School including the Nursery Unit

1.0 Introduction

This policy has been created in line with:

- DENI Circular 2016/27 "*Online Safety*"
- DENI Circular 2016/26 *"Effective Educational Uses of Mobile Digital Devices"*
- *360 Degree Online Safety Self-Review Tool for Schools* (May 2017) https://360safe.org.uk/Overview (Recommended by EA Belfast)
- DENI "*Safeguarding and Child Protection in Schools: A Guide for Schools"* (May 2017)

The policy is integrated into our Pastoral Care and Positive Behaviour Policy under the umbrella of St. Bride's PS Safeguarding and Child Protection Policy. It incorporates agreements on the acceptable use of (i) the internet and school-based digital technology and (ii) personal mobile technology.

This policy applies to all members of St. Bride's PS; pupils, teachers, peripatetic staff, volunteers, parents or carers and visitors who have access to and are users of our school ICT systems, both in and out of the school.

2.0 Definition of Online Safety

"Online safety means acting and staying safe when using digital technologies. It is wider than simply internet technology and includes electronic communication via text messages, social environments and apps, and using games consoles through any digital device. In all cases, in schools and elsewhere, it is a paramount concern."
DENI Safeguarding and Child Protection in Schools: A guide for Schools (May 2017)

"Online safety is about using digital devices in a smart but safe way. It means educating children and young people to act responsibly and keep themselves safe in the digital world."
C2K Support Materials on Fronter (May 2017)

2.1 Four categories of risks have been identified *(Safeguarding Board NI 2014)*

- **Content risks:** the child or young person is exposed to harmful material.
- **Contact risks:** the child or young person participates in adult initiated/child initiated online activity.
- **Conduct risks:** the child or young person is a perpetrator or victim in peer-to-peer exchange.
- **Commercial risks:** the child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs.

3.0 Whole School Approach

St. Bride's P.S adopts a consistent whole school approach to online safety. In St. Bride's P.S:

- Safeguarding including Online Safety is a key priority of all teaching and non-teaching staff, SMT, volunteers, visitors and the Board of Governors.
- All teaching and non-teaching staff can recognise and are aware of Online Safety issues.
- Online Training of teaching and non-teaching staff is appropriate and organised.
- Online safety messages are integrated across the curriculum for pupils in Nursery and all Key Stages.
- Online safety messages are distributed amongst pupils, staff, parents or carers and the wider community.
- Knowledge is shared amongst staff and there are good capacity building opportunities.
- There is on-going monitoring and evaluation of policy and practice.

3.1 Education of Staff

- All teaching and non-teaching staff of St. Bride's PS are familiar with our Online Safety Policy. Staff are trained to recognise and to be aware of online safety risks. Staff training on online safety risks forms part of St. Bride's PS Child Protection Training during the Baker Days in August and other relevant times as need arises. Online safety training is led by the ICT Co-ordinator, Mr Murray, in his role as SMT and because he has a higher level of expertise regarding online safety.
- Staff have read, understood and signed the St. Bride's PS Staff Acceptable Use Policy for C2k Managed Portable Devices (Appendix 6: EN094).
- Staff report any online safety incident to the Online Safety Co-ordinator, Mr Murray. (See *Procedures for Reporting and Dealing with Incidents Surrounding Breaches in the School's Online Safety Guidelines).* (Ref. 3.6)
- Importantly, if it is a safeguarding or child protection issue this will be reported to the Designated Teacher, Miss Joyce, or the Deputy Designated Teacher, Mrs Granleese. This is in line with St. Bride's PS Safeguarding and Child Protection Policy.
- Circulars relating to online safety e.g. DENI Circular 2016/17 'Online Safety', Circular 2016/26 Effective Educational Uses of Mobile Digital Devices, are emailed to all staff and they are saved for reference in the public folder.
- Staff share good practice in relation to online safety. In St. Bride's PS we recognise that some members of staff are more confident and competent users of digital technology and they are encouraged to share their good practice e.g. sharing of websites which promote online safety.
- Staff are aware that all digital communications with pupils and parents or carers should be on a professional level and only carried out using official school systems e.g. use of School Website, Fronter, Mangahigh and See Saw app.
- Internet use should be planned, task orientated and educational within a regulated and managed environment. It is best practice that pupils should be guided to sites checked as suitable for their use.
- Supervision is a key strategy. Pupils should have an adult present when accessing the internet and computers need to be positioned for adults to see the content on the screen.

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- Staff discuss with pupils the rules for responsible internet use as pupils need to be taught how to be internet wise and learn how to recognise and avoid potential risks. Staff recognise that pupils need to know how to respond to inappropriate material.
- Staff should act as good role models while using digital technologies, the internet and mobile devices.

3.2 Education of Pupils

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

- St. Bride's PS pupils are helped to understand and follow St. Bride's PS Online Safety Policy. They and their parents or carers annually sign our Pupil Acceptable Use of the Internet and School-Based Digital Technology including Mobile Digital Devices. (Appendices 2a, 2b and 2c)
- This Online Safety Policy covers pupil actions out of school if connected to members of our school community. St. Bride's PS pupils are taught the importance of adopting good online safety practice when using digital technologies out of school.
- Pupils are encouraged to adopt safe and responsible use of digital technology both in and outside school. All pupils are familiar with our Anti Bullying Policy which includes reference to online bullying.
- We adopt a preventative approach to online safety. We actively promote online safety messages for pupils on how to stay safe, how to protect themselves online and how to take responsibility for their own and others' safety. Childnet International SMART Posters (www.kidsmart.org.uk) are displayed around the school to help reinforce safety messages for pupils. Materials from outside agencies are also distributed to pupils for use in school or at home with their parents.
- Online safety lessons are integrated by staff across the curriculum for pupils in Nursery, Foundation Stage, Key Stage One and Key Stage Two. Standalone online safety lessons are incorporated into PDMU lessons, Safer Internet Day activities and school assemblies. Further learning opportunities are incorporated into ICT lessons in the ICT Suite e.g. podcasts, where the online safety messages are created by the learners themselves. We enter competitions organised by agencies such as EA/C2k.
- There are links to online safety websites in the Learning Zone section of our School Website that pupils access both in school and at home with their parents or carers. (http://www.stbridesps.org.uk/learning-zone/)
- Outside agencies e.g. NSPCC and the PSNI are used to reinforce the online safety messages from Years 2 - 7.
- St. Bride's PS pupils understand the importance of reporting abuse, misuse or access to inappropriate materials and know the procedures to follow. They are reminded of these during school assemblies.
- St. Bride's PS pupils are taught how to conduct online research safely and effectively and they understand the need to respect copyright when using material accessed on the internet.

- It is accepted that from time to time our pupils may need to conduct online research that would normally result in internet searches/pages being blocked e.g. when studying the negative effects of drugs e.g. smoking and alcohol for PDMU. In such a situation, staff can request that the ICT co-ordinator, Mr Murray, can temporarily remove these sites from the filtered list for the period of study.

3.3 Education of Parents or carers and Wider Community

St. Bride's parents or carers play a crucial role in ensuring that their children understand the need to use the internet and digital devices safely and in an appropriate way.

St. Bride's PS parents or carers are helped to understand and follow St. Bride's PS Online Safety Policy. They and their children annually sign our Pupil Acceptable Use of the Internet and School-Based Digital Technology including Mobile Digital Devices *(See Appendices 2a, 2b and 2c).*

Nursery and Year One parents or carers sign our *Consent Form for Digital Images* that allows their child's images to be used:

- Within the school for display purposes
- Externally for displays associated with the school
- By local, national, television and press
- On St. Bride's PS website,
- In 'The Bridge' School Magazine (where no names will appear with their image)
- On the St. Bride's PS Twitter account.

Parents have the choice to opt in or out of any of the above. Should a parent change their mind regarding permission for their child's image to be used, they are asked to put this in writing and inform the School Office so that records can be amended.

St. Bride's PS take every opportunity to help parents or carers understand online safety issues through parents' curriculum evenings, NSPCC workshops, curriculum newsletters, assemblies, termly newsletters, School Website, Fronter and information regarding national or local online safety campaigns and literature.

We advise St. Bride's PS parents or carers to take the following action when taking digital images of pupils in and around the school:

- Digital and video images may be taken at school events providing these are not uploaded to social media e.g. Facebook, Twitter, WhatsApp, Instagram, Snapchat

However:

- Taking digital and video images during swimming lessons and galas is not permitted.
- Taking digital and video images during Sacramental Celebration Events in St. Brigid's Church is not permitted. (This is in line with St. Brigid's Parish Safeguarding and Child Protection Policy.)

We believe that parents and carers have an essential role in the education of their children and in the monitoring of their on-line behaviours. Parents and carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure how to respond. The school will therefore help provide information and awareness to parents or carers through:

- The Internet and School Based Digital Technology Policy Agreement
- Personal Mobile Technology Form
- Termly Newsletters, which are sent home and are uploaded to the parent's section of the school website
- Fronter and School Website Learning Zones;
    - swgfl.org.uk
    - www.saferinternet.org.uk,
    - http://childnet.com/parents-and-carers
    - https://www.thinkuknow.co.uk/
- Curriculum Newsletters (located in the Tips for Parents or Reminder Section)
- Curriculum Nights in September
- Workshops from outside agencies e.g. NSPCC
- High profile campaigns e.g. Safer Internet Day (Term 2 each year)

3.4 Monitoring and Evaluating

As part of our Safeguarding Policy, St. Bride's PS keeps an Online Safety Risk Register where breaches of online safety are recorded. (This is kept by the Designated Teacher – Miss Joyce, together with the Safeguarding and Child Protection records in a locked filing cabinet.)

The Online Safety Policy is reviewed annually or earlier if deemed appropriate. This could be as a result of recent online incidents or new circulars from the DENI or the EA that require a change in St. Bride's PS Online Safety Policy.

This review is led by Mr Murray in his role as member of SMT and Online Safety Coordinator, who liaises with Miss Joyce in her role as Designated Teacher for Safeguarding and Child Protection. If changes are to be made, staff are consulted.

3.5 Managing of Personal Data

The School Principal (Mrs Quinn) and the School Secretary (Mrs Bannon) are both SIMS System Managers. They have access to the entire SIMS database. Both managers are able to approve various staff access to the different modules within SIMS e.g. teachers have access to their class details, the assessment coordinator has access to all modules relating to assessment. A copy of the St. Bride's PS Register of Access can be found on the Public Folder.

3.6 Procedures for Reporting and Dealing with Incidents Surrounding Breaches in the School's Online Safety Guidelines *(See flow chart in Appendix).*

(Adapted from South West Grid for Learning (SWGfL) Online Safety)

St. Bride's PS, in line with our Safeguarding and Child Protection Policy, has robust channels of communication in place for reporting online safety issues. Pupils and staff know who they can turn to if there is a problem. Instances relating to Safeguarding and Child Protection should be communicated to the designated teacher Miss Joyce, DT in the Nursery Ms Ward or deputy designated teacher Mrs Granleese. More advice is available if required in the Safer Internet Area within Fronter, a component part of the C2k NI service. This area is updated regularly.

In cases of Internet abuse, or where a pupil is at risk, our safeguarding and child protection procedures will be implemented.

The school will deal with such incidents in line with the recommendations of SWGfL which is outlined below. The school will, if necessary; inform parents or carers of incidents of inappropriate Online Safety behaviour that takes place in our school, or outside school if it involves members of our school community.

If there is an online safety incident, the action taken depends on whether unsuitable materials were involved or if there were illegal materials or activities found or suspected.

In the first instance if unsuitable material is found:

- This is reported to the Online Safety Co-ordinator Mr Murray.
- The Online Safety Co-ordinator assesses the material and discusses it with the persons involved (staff or pupils) and decides upon an appropriate course of action.
- Mr Murray will record details in the Online Safety Risk Register and may if necessary consult with the DT or DDT. If appropriate the DT or DDT will consult with the Safeguarding and Child Protection Team at the Education Authority.
- Mr Murray liaises with SMT to discuss the incident.
- Following this assessment, the policy may be reviewed and changed if lessons have been learned.

In the second instance, if illegal materials or activities are found or suspected, *which pose no immediate risk to pupils*; the above procedures will be followed and it will be reported to CEOP (Child Exploitation and Online Protection.)

- The evidence must be secured and preserved.
- The school then awaits a response from CEOP or from the police.
- If no illegal activity or material is confirmed, we revert to our internal procedures.

If the incident is more serious:

- If illegal activity or materials are confirmed, police or relevant authorities complete their investigation and seek advice from relevant professional bodies.
- In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action.

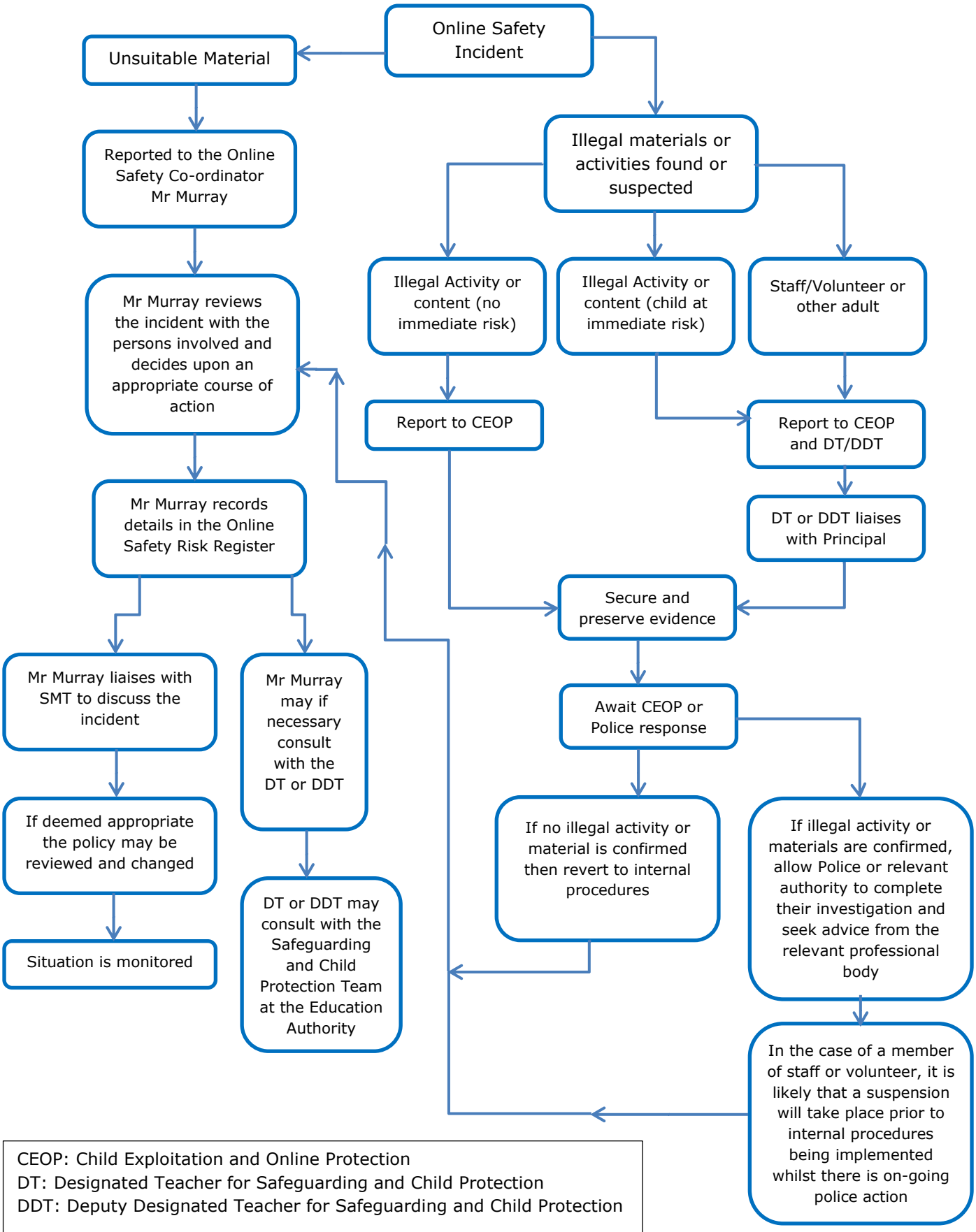
If illegal material or activities are found, or are suspected, that pose immediate risk:

- The member of staff or Mr Murray reports this to CEOP and to the Designated Teacher or the Deputy Designated Teacher who follow St. Bride's PS Safeguarding and Child Protection Procedures.
- The evidence must be secured and preserved.
- The school then awaits a response from CEOP or from the police.
- If illegal activity or materials are confirmed, police or relevant authorities complete their investigation and seek advice from relevant professional bodies.
- In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures being implemented whilst there is on-going police action.

St Bride's Primary School

Procedures for Reporting and Dealing with Incidents Surrounding Breaches in the School's Online Safety Guidelines

(Adapted *from South West Grid for Learning (SWGfL) Online Safety)*



CEOP: Child Exploitation and Online Protection
DT: Designated Teacher for Safeguarding and Child Protection
DDT: Deputy Designated Teacher for Safeguarding and Child Protection

4.0 Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within St. Bride's PS.

4.1 The Board of Governors

The Board of Governors are responsible for the adoption of the Online Safety Policy and for reviewing the effectiveness of the policy. The Link Governor for ICT (Ms Crossan) will also be the Online Safety Governor. Her responsibilities will include:

- Attending meetings with the ICT Coordinator Mr Murray whose role also includes that of Online Safety Co-ordinator
- Discussing Online Safety incident logs where necessary
- Reporting back if necessary to relevant Governors e.g. if it's a Safeguarding and Child Protection issue to Mrs Agnew (the link governor for Safeguarding and Child Protection)

4.2 The Principal

The Principal, Mrs Quinn, has a duty of care for ensuring the safety (including online safety of members of the school community) though the day to day responsibility for online safety will be delegated to the ICT Co-ordinator, Mr Murray. Mrs Quinn has also the responsibility for managing emails e.g. if emails are quarantined for a particular reason then she liaises with C2k to have them released.

The Principal and Senior Management Team are responsible for ensuring that Mr Murray, the ICT Coordinator, and other relevant staff, receive appropriate training to enable them to carry out their online safety roles and train their colleagues, as relevant.

4.3 The Online Safety Co-ordinator (Mr Murray)

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies with the Designated Teacher for Safeguarding and Child Protection, Miss Joyce
- Ensures that all staff are aware of procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff regularly including during safeguarding and child protection staff training days
- Liaises with Education Authority (EA) Belfast
- Liaises with C2K technical staff
- Receives reports of online safety incidents and completes a log of incidents in the Online Safety Risk Register which can be used to inform future online safety developments
- Attends relevant meetings e.g. cluster meetings, C2k, Fronter, iTeach Conferences
- Reports regularly to Senior Management Team
- Maps and review our Online Safety curricular provision – ensuring relevance, breadth and progression.
- Monitors the impact of Online Safety education in our school and if necessary to fill any gaps.
- Raises and manage new initiatives including annual initiatives such as anti-bullying week and Safer Internet Day
- Produces, monitors and reviews St. Bride's PS Online Safety Policy

- Monitors network incident logs
- Monitors incidents and establish the best way of dealing with them
- Engages our school community including parents or carers and the pupils about the online safety provision – working together to benefit all
- Monitors and reviews St. Bride's PS filtering policy and approve requests for filtering changes.
- Monitors improvement actions identified through use of the 360 Degree Safe Self-Review tool

4.4 Service Providers, Technical – infrastructure / equipment, filtering and monitoring

St Bride's PS has a managed ICT service provided by C2k. It is our responsibility to ensure that the service provider (C2k) carries out all the online safety measures that would otherwise be the responsibility of the school.

C2k regularly monitor our network for any misuse or attempted misuse which can then be reported to the Principal or Online Safety Co-ordinator. C2k ensures that the school meets recommended technical requirements. They regularly review and audit the safety and security of our school system. Servers, wireless systems and cabling is securely located and physical access is restricted. All users have clearly defined access rights to school technical systems and devices (See Register of Access List). All users are provided with a username and secure password by the Network Manager (Mr Murray) who keeps an up to date record of users and their usernames. Staff and pupils are responsible for the security of their username and password and will be required to change their password every 3 months. The 'C2k Manager' password for our school network used by the Network Manager (Mr. Murray) is available to the Principal (Mrs Quinn).

The managed service provider (C2k) is aware of:

- DENI Circular 2016/27 "*Online Safety*"
- DENI Circular 2016/26 *"Effective Educational Uses of Mobile Digital Devices"*

A second wifi system, 'Classnet', provided by iTeach also exists in the Derryvolgie and Ashleigh sites. It is a filtered, safe and secure wifi system which complies with all statutory guidelines. It is built around the Cyren filter system, ensuring online protection and flexibility when necessary. iTeach regularly provide guidance, technical support and updated relevant risk assessment documents to St. Bride's PS

Effective Educational Use of Mobile Digital Devices
(Including laptops, tablets, smart phones, iPods, memory sticks, gaming consoles)

5.0 Introduction to mobile digital devices

Mobile digital devices in school provide both educational opportunities for learners and teachers as well as management challenges which are different than those afforded by desktop computers.

5.1 Rationale

St. Bride's PS are currently operating a small-scale iPad 'Roll Out' beginning with Nursery and Foundation Stage. There will be continued investment in associated professional development for staff which is required to share best practice, to evaluate the benefits and long-term success.

5.2 Guidelines for Pupils and Staff on the use of Mobile Digital Devices

5.21 Pupils

St. Bride's PS recognises that whilst mobile digital devices can benefit learning and teaching inside and beyond the classroom there is a risk of distraction from school work and a risk to online safety. In order that the safety of all pupils is protected, personal mobile phones, cameras, iPods and game consoles are not permitted to be used by pupils on the school premises. Should parents feel that their child requires a mobile phone to ensure their safety while travelling to and from school, they must apply in writing to the Principal. If permission is granted, the mobile device will be handed in to Vice Principal's Office at the beginning of the school day where it will be secured until the end of the school day.

5.22 Staff

During teaching time, playground supervision and meetings, mobile phones will be switched off or on silent mode. Except in urgent or exceptional circumstances mobile phone use is not permitted during teaching time, playground supervision or at a meeting. However, we recognise that some non-class based teachers may need to be contacted using mobile phones and in these cases phones will be switched on.

In the Nursery, the Head of Nursery will use her mobile phone for the purpose of connecting to an outdoor speaker for the enhancement of music provision. All songs are monitored for appropriateness of content prior to being used for teaching and learning activities.

6.0 Enhancing and Transforming Learning and Teaching (Circular 2016/26)

The following four categories are ways in which mobile digital devices may be integrated significantly to enhance and transform aspects of learning to real advantage:

- Capturing and collecting information and experiences across a variety of settings, through photos, audio and video recordings, numerical and text entry.
- Communicating and collaborating with others via Fronter, Seesaw App in the Nursery and email.
- Consuming and critiquing media including music, photos, videos, games and text documents.
- Constructing and creating personal forms of representation and expression through edited photos and videos, sketches, podcasts, blogs etc.

In St. Bride's PS we have some specific learning activities which mobile learning can valuably enable. Pupils can:

- **Review and reflect:** pupils capture audio, imagery and video during lessons, use these in plenary sessions e.g.in structured play to reflect on an activity, consider the key elements learned, how these fit into wider subject or topic pictures and how ideas might be used or taken further outside the classroom.
- **Think forward:** pupils access future topic material via the Internet and capture relevant thoughts or ideas (research) to contribute to discussions or presentations in class or through on-line discussions.
- **Listen to my explanations:** pupils record audio when they are completing class work and these verbal explanations are listened to by teachers and peers.
- **Snap and show:** pupils capture imagery, which can be copied to our network and accessed through a computer or interactive whiteboard screen, for wider pupil discussion.
- **This is what I've done and how I've done it:** pupils create presentations using mobile technologies for particular activities, which are recorded and made accessible on our school website for teachers and parents to see.
- **Tell me how I could improve this:** pupils can share their work in multimedia formats with peers, teachers or trusted adults to seek comments, evaluative feedback, assessments of their work and ideas to improve their work.

7.0 Guidelines for Using iPads for Staff and Pupils

- Users must use protective covers/cases for their iPad.
- The iPad screen is made of glass and therefore is subject to cracking and breaking if misused. Never drop or place heavy objects (books, laptops, etc.) on top of the iPad. Only a soft cloth or approved laptop screening solution is to be used to clean the iPad screen.
- Do not subject the iPad to extreme heat or cold.
- Do not store or leave unattended in vehicles.
- Jail breaking is the process which removes any limitations placed on the iPad by Apple. Jail breaking results in a less secure device and is strictly prohibited.
- In the case of loss, theft or other damage occurring outside of school, users accept full responsibility to repair, replace or make good the iPad to its original state.

7.1 Acceptable Use of iPads

- Use of the iPad should be considered the same as any other technology tool provided by the school.
- The user will abide by St. Bride's Online Safety Policy and Pupil Acceptable Use of the Internet and School-Based Digital Technology Including Mobile Digital Devices with regard to iPad usage.
- Staff should email the ICT Co-ordinator a list of suitable apps which they require. These will be researched and ICT Co-ordinator will consult the Principal/Vice Principal before purchasing.
- All apps will meet the requirements of St. Bride's Online Safety Policy.
- Staff should inform the ICT co-ordinator of any apps that do not meet safety requirements. These apps will be removed from the device.

- The iPad will not be synched or attached to your home or personal computer. Only school accounts will be used.
- Do not use the device to store personal documents such as video or audio material other than which is directly related to your school needs.
- Use of the camera only permitted in line with the Safeguarding and Child Protection Policy. All images are not allowed to be stored on the device. Images should be uploaded ASAP to the school network and deleted from the device.
- You will not remove profiles or restrictions placed on the device.

7.2 Security of iPads

Staff should unsure that:

- A four-digit secure passcode is used on the teachers' devices and this passcode will be provided when necessary to the school management team.
- The passcode of the device is held private to the teacher and classroom assistant and is not divulged to pupils.
- Pupils use the iPad for curricular purposes only in a controlled environment in the presence of a member of staff.

7.3 Advice on Safeguarding and Maintaining iPads

- iPads should be charged and ready to use in school every day.
- When the iPads are charging they will be saving all information onto iCloud.
- Any items that are deleted from the iPad cannot be recovered.
- The memory space on the iPads, are limited, so only school documents/materials should be stored.
- Each member of staff should know the number of their iPad. A copy of this is held by the ICT Co-ordinator. It is staff's responsibility to ensure that the iPad is kept safe and secure. IPads should not be shared or tampered with in any matter. If an iPad is found unattended, it should be returned to the ICT co-ordinator.
- If the iPad is lost, stolen or damaged, Mr Murray, the ICT Co-ordinator should be notified. Ipads that are believed to be stolen can be tracked through iCloud.

7.4 Prohibited use of iPads, Smart Phones, iPods etc.

- All material on the iPad must adhere to St. Bride's Online Safety Policy. Users are not permitted to send, access, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
- St. Bride's internet/ email accounts may not be used for financial or commercial gain or illegal activity.
- Violating Copyrights - users are not allowed to have music and install apps on their iPad.
- Cameras - users must use good judgement when using the camera on iPads. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any misuse of mobile digital devices e.g. camera in toilets or changing room, regardless of intent, will be treated as a serious violation and will be dealt with in line with our Safeguarding and Child Protection Policy.

- Any misuse of mobile digital devices e.g. smart phones on online group chat forums will be dealt with in line with our Positive Behaviour Policy. Parents will be informed.
- Images of people may only be used with the permission of those in the photograph.
- Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of a member of the Senior Management Team.
- Use of the camera and microphone, by pupils, is strictly prohibited unless permission is granted by a teacher.
- No user may gain access to another user's accounts, files or data.
- No user may attempt to destroy hardware, software or data.
- Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.
- Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school.
- All users should be aware of and abide by the guidelines set out in St. Bride's P.S Online Policy.
- The Principal and Designated Teacher reserve the right to confiscate and search an iPad to ensure compliance with this Online Safety Policy.

Appendix 1a

St. Bride's Primary School

Parents Acceptable Use of Digital Images Agreement

Dear Parents

As part of our Safeguarding & Child Protection Procedures we ask parents to give written consent to allow their child's images to be used-

1. within the school for display purposes
2. externally for displays associated with the school
3. by local, national, television and press
4. on St Bride's PS website, in the Bridge school magazine (no names will appear with their image) and on the school Twitter account.

We advise you that:

- Digital and video images may be taken at school events providing these are not uploaded to social media e.g. Facebook, Twitter, WhatsApp

However:

- Taking digital and video images during swimming lessons and galas is not permitted
- Taking digital and video images during Sacramental Celebration Events in St. Brigid's Church is not permitted. (This is in line with St. Brigid's Parish Safeguarding and Child Protection Policy.)

M R Quinn
Principal

Child's Name _____ Class/Teacher _____

I allow my child's image to be used for (please tick)

- □ within the school for display purposes
- □ externally for displays associated with the school
- □ by local, national, television and press
- □ on St Bride's PS website, in the Bridge school magazine (no names will appear with their image) and on the school Twitter account

Please note if you do not wish for your child's image to be used in any of the above categories you have the option to opt out by not ticking the box.

I acknowledge the advice given re. digital and video images being taken.

Signed: _____
Parent /Guardian

Appendix 1b **St. Bride's Nursery Unit**

Parental Digital Image Acceptance Form

Dear Parent,

As part of our Child Protection Procedures, we are asking parents to sign to give permission for their children's images to be used;-

1. Within the school for display purposes
2. Externally for displays associated with the school e.g. school magazine
3. By local, national, television and press
4. on St Bride's PS website, in the Bridge school magazine (no names will appear with their image) and on the school Twitter account.
5. Within the Seesaw app (see note below)

In order to strengthen our communication with parents, we will be using an app called Seesaw to keep parents up-to-date with their child's learning profile; parents will have an opportunity to log on to their own child's profile which will contain photographs of their children at play along with a short caption. We hope this will allow both parent and child to have a more meaningful dialogue about their play experiences and/or learning goals. Due to the nature of the nursery day, it is likely that there may be images of other children alongside or in the background. In line with the whole school Child Protection Policy, no parent may copy/screenshot images where other children are present, and upload or transmit to any third party. In St. Bride's Nursery, only parents may log on and connect to the Seesaw app.

As part of our child protection policy, parents using the Seesaw app must undertake that any other family member they invite to view their own child's learning profile, is aware of the above policy.

M R Quinn (Principal)

Ms Ward (Head of Nursery)

I allow _____(child's full name) image to be used for (please tick)

- ☐ within the school for display purposes
- ☐ externally for displays associated with the school
- ☐ by local, national, television and press
- ☐ on St Bride's PS website, in the Bridge school magazine (no names will appear with their image) and on the school Twitter account
- ☐ Within the Seesaw app

Please note if you do not wish for your child's image to be used in any of the above you have the option to opt out by not ticking the box.

Class/ Teacher_____ Signed_____

Appendix 2a

St. Bride's Primary School Pupil Acceptable Use of the Internet and school-based digital technology including mobile digital devices

Dear Parents/Carers

This form relates to the pupil Acceptable Use Agreement which is attached. Keep this cover note for your own records.

Please read and discuss this agreement carefully with your children and sign the relevant section attached overleaf to show that you have read, understood and agree to the rules included in our Acceptable Use Agreement.

Unfortunately, if the agreement is not signed, access will not be granted to school systems.

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Our pupils have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure that:

- Our pupils will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- St. Bride's PS systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

Many thanks

MR Quinn

School Principal

St. Bride's PS

Appendix 2b ***St. Bride's Primary School Pupil Acceptable Use of the Internet and School-based Digital Technology Including Mobile Digital Devices (Nursery, Foundation and Key Stage 1)***

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers or iPads.
- I will log on using my username and password and I will keep it private.
- I will not access other people's files without permission.
- I will only use the computers and iPads for school work and homework.
- I will only do activities that a teacher or suitable adult has told or allowed me to do.
- I will take care of the computer and iPads.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will use the internet only when an adult is present.
- I will not bring a laptop, tablet, smart phone, iPod, memory stick, gaming console to school without permission.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer or iPad.

Year Group	Pupil Signature	Parent/Carer Signature	Date
Primary 1			
Primary 2			
Primary 3			
Primary 4			

Appendix 2c

St. Bride's Primary School Pupil Acceptable Use of the Internet and school-based digital technology including mobile digital devices

(Key Stage 2)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers or iPads.
- I will log on using my username and password and I will keep it secret.
- I will not access other peoples' files without permission.
- I will only use the computers and iPads for school work and homework.
- I will only do activities that a teacher or suitable adult has told or allowed me to do.
- I will take care of the computer and iPads.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will access the internet only when an adult is present.
- I will not bring a personal digital device (including laptops, tablets, smart phones, iPods, memory sticks, gaming consoles) to school without permission.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer or iPad.
- I will send messages that are polite and responsible. If I send inappropriate messages or pictures, my parents will be contacted by the school.
- I will report any inappropriate material or unpleasant messages.
- I understand that St. Bride's PS has full access to all my files and monitors my use of the internet, digital devices and communications
- I will not use internet chat rooms in school.
- I will be aware of 'Stranger Danger' if I am communicating online.
- I will not give out or pass on personal information or passwords e.g. names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details.

Year Group	Pupil Signature	Parent/Carer Signature	Date
Primary 5			
Primary 6			
Primary 7			

Appendix 3

C2k Acceptable Use Policy

DELIVERING TECHNOLOGY FOR LEARNING

Terms & Conditions

C2k Exchange provides you with a protected online area. It includes access to your C2k email, a document area where all C2k service documents are stored, a discussion area where you can discuss C2k services with other school staff and C2k staff, a news area containing articles on Northern Ireland ICT in education stories, best practice case studies, and a contact area providing information on other ways to communicate with C2k.

Your C2k Exchange access is provided subject to the following terms of use:

1. You must use C2k Exchange in a professional manner consistent with the rules of behaviour governing education sector employees.

2. You must comply with all relevant laws when using C2k Exchange/email. You may not upload, store or distribute any inappropriate or illegal material either through C2k Exchange or by email.

3. By submitting any contribution to C2k Exchange you warrant that you are its author; that you have the right to make it freely available to C2k Exchange; that it does not infringe any law; and that you will indemnify C2k against all legal fees, damages and other expenses that may be incurred should you breach such warranty. Note that for any work made in the course of employment, copyright ownership rests with your employer.

4. User contributed content is provided as is and without warranty from C2k of any kind. C2k may not be held responsible for any defect or inaccuracy in any content held within C2k Exchange. In the event of any materials held in C2k Exchange becoming subject to complaint, C2k will make best efforts to withdraw such material at once pending investigation of the matter.

5. C2k will not be liable against any loss in respect of material uploaded to C2k Exchange by any school/organisations, users or guest users.

6. Content within C2k Exchange may contain hyperlinks to external resources. C2k is not responsible and shall not be liable for the availability, nature or use of any external content or the policies of linked websites. You must not offer a link to any site that contains direct marketing/commercial advertising, inappropriate or infringing content.

7. Personal information about any living person must not be published through C2k Exchange without express prior permission from the person concerned.

8. The names, images and logos identifying C2k, C2k Exchange or third parties and their products and services are subject to copyright, design rights and trade marks and may not be copied or used without permission. All Rights Reserved.

9. Where inappropriate use of C2k Exchange is detected, disciplinary action may be taken against the user concerned to reduce or remove C2k Exchange access privileges and a report submitted to any appropriate authority.

10. The views expressed in C2k Exchange discussions are those of the individual contributors and do not necessarily represent C2k/LNI.

11. C2k Exchange is committed to safeguarding each user's privacy online. Any user information stored by the system is that provided by his/her school/organisation to enable the user to make use of the system, and that which is generated by any system tracking. This information will be held securely and processed only in conformity with the UK Data Protection Act 1998. While normal privacy is respected and protected by password controls, as with the Internet itself, users must not expect files stored on LNI servers to be absolutely confidential. The users' right of privacy is balanced against C2k's right to gather usage information (e.g. where required by law, system performance and service improvement).

12. By using C2k Exchange you are considered as understanding and agreeing to the contents of the terms published here (and any revisions/additions as C2k may post here at any time).

Appendix 4 – Acceptable Use Policy for C2k Managed Portable Devices

Information sheet EN094

Acceptable Use Policy for C2k Managed Portable Devices

School Name:		**DE Number:**	
	Device Serial Number		
Conventional Laptop (HP ProBook 450)		Convertible laptop (HP Pro x2 612)	

This policy should be signed by any member of staff who will take a devices away from the school.

I understand that I am the *nominated member of staff* for this device, and I agree that:

(Please tick each box)

Ownership of this device rests with C2k, and that I may retain it for school use while in the employment of this school.	☐
Use of device, in and outside school, is subject to the school's AUP.	☐
Logon to the device is only possible with a valid C2k Username and password, and that disclosure of individual C2k Username and password represents a security breach.	☐
The facility to install software should only be used to load resources which are licenced and which are appropriate for school needs. In particular, device users may not install Windows updates or any hacking tools and should not switch off Windows firewall	☐
The device is insured by C2k only while inside school for thefts or malfunction and not for accidental damage. If the device is removed from school, alternative insurance cover must be provided (or replacement liability accepted) both for car and other location.	☐
Antivirus software is provided and automatically updated in school or when connected to the Internet. **This protection must be kept up to date if the device has not been connected to the school network or the Internet for more than two weeks.**	☐
The device may be used outside school for Internet use with any Internet Services Provider (ISP). ***It is the responsibility of device users to ensure that confidential information is not saved to the portable device.***	☐
The device should not be given or lent or used by anyone other than the nominated member of staff when outside school.	☐
If the device is lost or stolen, the school should be notified immediately, or during school holidays, the C2k Helpdesk (0870 6011 666).	☐
The device must be returned to school if the nominated member of staff ceases employment with the school.	☐

Signature: Date:

May 2015 1 of 1 http://www.c2kexchange.net