



*Together Everyone
Achieves More*

Internet Safety and Acceptable Use Policy

St Patrick's Primary School Portrush

Policy No:	Signed by Chair of BOG	Date ratified by BOG
7	Mr Andrew McGreevy	August 2018
Agreed date	Review date	Person responsible for review
February 2021	February 2022	Principal Mr. Dinsmore

Contents

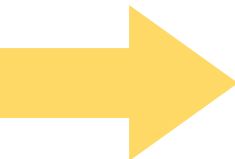
Internet Opting Out Policy	1
Who is this Policy for?.....	1
Context	1
Effective Use of the Internet in the Curriculum.....	2
Internet Safety Awareness	2
Measures for Safe Practice.....	2
Safe Practice Measures for Pupils	2
Safe Practice Measures for Staff	3
Sanctions	5
School Website and Friends of St Patrick's Facebook Page	5
Social Media	6
Staff Use of Social Media	6
Discussion of the School and School Community on Social Media.....	6
Cyber Bullying	7
Help and Advice for Parents/Carers on Children's Use of the Internet at Home	8
Accessibility Statement	8
Policy Record and Review Date.....	Error! Bookmark not defined.
Appendix 1 - Code of Conduct: Acceptable Use of the Internet	9

Translate this document at:

Przetłumacz ten dokument na:

<https://translate.google.co.uk/>

Преведете този документ на адрес:



Internet Opting Out Policy

The school will operate an opting out policy for the use of Internet.

Parents/carers must inform the school if they do not wish their children to access the MySchool internet for school related activities.

Who is this Policy for?

1. This Internet Safety and Acceptable Use Policy is to inform, guide and assist the entire school community. This includes staff (teaching and non-teaching), parents/carers, children and other public bodies involved in the provision of education or safeguarding children.

Policy Links

2. This Policy, where appropriate, must be considered and implemented in conjunction with the Pastoral Care, Positive Behaviour Management and Safeguarding Children Policies.

Context

3. The internet is essential and positive element in daily life for education, business and social interaction. At St. Patrick's Primary School, we provide children with access to the internet as part of their learning experience. The purpose of the internet is to raise educational standards, to promote pupil achievement and to support the professional work of staff.
4. At St Patrick's we provide children the necessary information and skills to keep themselves safe when using the internet. However, it is also important to be aware that the school alone cannot protect children from all risks associated from the Internet, particularly when outside our carefully controlled ICT environment. Staff, Governors, parents and pupils all have to take responsibility for the use of technology and the internet.
5. This document sets out the policy and practices for the positive, safe and effective use of the internet in St. Patrick's Primary School.

Effective Use of the Internet in the Curriculum

6. The use of school ICT resources by pupils must only be used in support of the aims and objectives of the school and teaching the Curriculum.

Internet Safety Awareness

For Pupils

7. Rules for the acceptable use of the Internet must be discussed with all pupils at the start of each year and displayed in areas used for ICT.
8. When available external agencies, such as the local PSNI will support ICT safety in special class exercises.

For Staff

9. The principal is responsible for keeping himself and other staff informed and updated on issues relating to Internet safety.

Internet Safety Awareness for Parents/Guardians

10. The Internet Safety Policy and Code of Practice for pupils must be sent to parents to parents/carers every year along with Safeguarding and Child Protection Policy.
11. Parents/carers are also welcome to contact the school to make an appointment to discuss internet safety or to view the school's internet safety arrangements

Measures for Safe Practice

Safe Practice Measures for Pupils

12. Pupil access to the Internet is through a monitored and filtered service provided by C2K, which ensures educational use of resources is safe and secure, while protecting users and systems from abuse. However, rigorous as these measures are, they can never be 100% effective and neither the school nor C2K can accept liability for images, words or other material that might get through the C2K filter.

13. In addition to the C2K filter the following key measures have been adopted by St Patrick's Primary School to minimise the risk of pupils accessing inappropriate material:

- a) pupils using the Internet are only allowed to work in highly-visible areas of the school;
- b) all online activity is supervised and based on appropriate educational objectives;
- c) pupils will, where appropriate, use sites pre-selected by the teacher and appropriate to their age group;
- d) the school's Code of Practice (Appendix 1) for use of the Internet and other digital technologies is made explicit to all pupils and displayed prominently in ICT areas; and
- e) All pupils are educated in the safe and effective use of the Internet.

14. During school hours, pupils are forbidden to play computer games, unless specifically assigned by the teacher. Social networking sites such as Facebook are not available to pupils as these are filtered and monitored by C2k.

15. Pupils are forbidden from using personal internet enabled devices in the school premises (mobile phones can only be used in accordance with the Mobile Phone Policy in the Safeguarding and Child Protection Policy). Staff may not use their mobile phones to record images or access internet during school. Authorised devices are available in school. Each teacher has an assigned iPad.

16. Any attempts to bypass filtering or to access inappropriate or illegal material by the children may be dealt in line with our Positive Behaviour Management policy.

Safe Practice Measures for Staff

17. Pupils accessing the internet must be authorised by a teacher and supervised by an adult at all times. The authorising teacher is responsible for ensuring supervision is in place.

18. All pupils and staff must be made aware, consult with and agree the schools Acceptable Use policy. These must be displayed in ICT areas.
19. Where a parents/carer was withdrawn permission for their child to use the internet the class teacher will ensure appropriate measures are put in place to restrict access.
20. Teachers must ensure their year group has recommended websites available under "Favourites". Any additional websites used by pupils must be checked beforehand by the teacher to ensure there is no unsuitable content and that material is age-appropriate.
21. Depending upon their seriousness, deliberate or accidental access to inappropriate materials or any other breaches of the school Code of Practice must be reported at the earliest opportunity to the Principal in writing.
22. Staff should only use school ICT systems and resources for all school business. It is acknowledged that sometimes lessons are prepared on personal devices at home. This should be avoided wherever possible.
23. Staff must not download, copy or use any materials in breach of copyright or intellectual property rights.
24. Photographs of pupils should be taken with a school ipad only. The images must remain in school, be stored in a centralised area on the school network, and be accessible only to teaching staff. Staff must not take photographs on their own Mobile Phones. Images must be retained in accordance with the Data Protection Act¹
25. All use of the Internet must be on sites appropriate to a primary school.
(Teachers are reminded that the C2K system tracks Internet use and records every site visited. The system also logs emails and messages sent and received by individual users);

¹ Or, when in force, the Data Protection Regulations.

The fifth data protection principle requires that staff must:

- review the length of time you keep personal data;
- consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

26. Any attempts to bypass filtering or to access inappropriate or illegal material may be dealt with as a disciplinary matter.
27. Emails may occasionally be blocked because of the C2K filtering system. If access is required, this must receive authorisation from the Principal.
28. Only appropriately licensed software may be added to the school's network. C2K's permission is required for the connection of additional devices.
29. The usernames and passwords of leavers (and anyone under investigation) will be disabled promptly; accounts must not be created for fictitious staff;
30. School systems may not be used for unauthorised commercial transactions.

Sanctions

31. Depending upon their seriousness, any incidents of technology misuse which might arise will be dealt with in accordance with the school's Positive Behaviour Management Policy by the class teacher or the Principal. Serious misuse may result in a temporary or permanent ban of Internet use. Incidents involving Safeguarding/Child Protection issues will be dealt with in accordance with school Safeguarding Children Policy.

School Website and Facebook Page

32. The school website and the Facebook Page keep the School Community informed of events, updates and achievements. They also serve an important role in promoting the school. To ensure the best use of these tools and to ensure child protection staff must ensure:
 - i. names of students must not accompany photographs;
 - ii. home information and email identities must not be included - only the point of contact to the school i.e. school telephone number, school address and email address should be used;
 - iii. group photographs must not contain a names lists; and
 - iv. work displayed will be of the highest quality and reflect the status of the school.

- v. Only teaching staff are permitted to post on School Website or a social media platform e.g. Facebook and must always have prior consent of the Principal.

Social Media

- 33. There is a wide range of social media which allows pupils and the wider school community to connect and communicate. These can have both positive and important role, such as keeping the school community informed of events and developments in the school or highlighting the schools successes.
- 34. Social Media can also have a negative impact for example the inappropriate use for content or language which is linked to the school or **cyber bullying**.
- 35. Social networking applications include, but are not limited to: Blogs, Online discussion forums, Collaborative spaces, Media sharing services, 'Microblogging' applications, and online gaming environments. Examples include Twitter, Facebook, Windows Live Messenger, YouTube, Flickr, Xbox Live, Blogger, Tumblr and comment streams on public websites such as newspaper sites.

Staff Use of Social Media

- 36. Staff must exercise caution when using information technology and be aware of the risks to themselves and others. Regard must be given to the schools' Internet Safety and Acceptable Use Policy and Safeguarding and Child Protection Policy, including the Code of Conduct, at all times both inside and outside of work.

Discussion of the School and School Community on Social Media

- 37. Many people use social media to communicate with friends, colleagues, family members and other people about things that happen in and around the life, including in the school community.
- 38. Other schools in Northern Ireland have experienced problems when members of the school community, such as pupils/parents/carers, have raised concerns

on social media about the progress of their child, the behaviour of another child, a dislike of a staff member or the actions of the school, etc.

This practice is not acceptable at St Patrick's Primary School, as it does not serve the interests of the children or the school. Anyone with concerns are encouraged to use official channels which are best suited to resolve any issues professionally and as quickly as possible.

Cyber Bullying

39. Bullying doesn't just happen in the playground. Cyberbullying – or bullying via digital technologies like mobile phones and computers – is a different threat to children. It can be harder to spot and more difficult to stop than 'traditional' bullying.

40. Cyber Bullying is defined² as the repeated use of electronic communication by a pupil or a group of pupils against another pupil or group of pupils, with the intention of causing physical or emotional harm to that pupil or group of pupils.

41. The school does not tolerate bullying in any form and will deal with all instances of bullying constructively, but with the upmost seriousness in accordance with the Positive Behaviour Policy and Safeguarding Children Policy³.

42. Parents/carers have a responsibility to help the school addressing bullying behaviour, particularly if it involves Cyber Bullying to ensure the appropriate use of the internet by children outside school to help prevent cyber bullying.

² From the Addressing Bullying in Schools Act (Northern Ireland) 2016.

³ Or, if appropriate, staff grievance and/or disciplinary procedures.

Help and Advice for Parents/Carers on Children's Use of the Internet at Home

43. More help and advice on Cyber Bullying, or children's safe use of the internet at is available on the [NI Direct Website](https://www.nidirect.gov.uk/information-and-services/your-childs-health-and-safety/internet-safety)⁴.

44. Advice is also available from the [NSPCC Website](https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/)⁵.

Accessibility Statement

45. In developing this policy every effort to make it easy to understand. **If you need help to read or understand this please contact us, we want to help.**

46. The following steps have been taken to make the document accessible. We have:

- a) used clear and direct language wherever possible;
- b) used correct tagging, formatting, numbering and use of headings for e-readers; and
- c) followed [government guidance](#) on document accessibility.

47. If you need this document in another form, such as large print or you have any suggests as to how we could improve the accessibility please contact the school office.

⁴ <https://www.nidirect.gov.uk/information-and-services/your-childs-health-and-safety/internet-safety>

⁵ <https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/>

Appendix 1 - Code of Conduct: Acceptable Use of the Internet

- A. At St Patrick's Primary School all pupils are responsible for their own behaviour on the Internet. This includes materials they choose to access, and any language they use.
- B. Pupils using the internet must not deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.
- C. Pupils must not to use any rude language in their email communications and contact only people they know or those the teacher has approved. It is forbidden to be involved in sending chain letters.
- D. Pupils must ask permission before accessing the Internet.
- E. Computers must only be used for schoolwork and homework unless permission has been granted otherwise.
- F. When appropriate, homework completed at home, may be brought in on pen-drive, but this will have to be approved by the teacher and virus scanned before use.
- G. Personal printing is not allowed (e.g. pictures of pop groups / television characters).
- H. Pupils must never share personal information such as telephone numbers and addresses.
- I. Pupils must never make arrangements to meet someone unless this is part of an approved school project.
- J. Pupils consistently choosing not to comply with these expectations will be denied access to Internet resources.
- K. The Principal may check My computer files and may monitor the internet sites I visit.