

St. Canice's Internet Acceptable Use & Digital Device Safety Policy

Mission Statement

St. Canice's is committed to the use of electronic resources and technology to enhance the administrative, teaching and learning opportunities for students and staff. Therefore, students and staff are encouraged to utilise these resources within the guidelines set forth in the Internet Acceptable Use & Digital Device Safety Policy. Keep in mind all such usage should apply directly to school administration and to the implementation of the school curriculum. Mobile phones can be intrusive and distracting in school. There may also be possible harmful effects due to frequent use and children could be particularly vulnerable in this regard. They can also contribute to cyber bullying. Other communications devices such as game consoles, psps, ipods, etc are also capable of being used for cyber bullying and/or online abuse. Strategies must be put in place to reduce the intrusiveness of unauthorised technology in a school situation. The use of mobile phones and other electronic games/devices contravenes the provision of a safe and secure school environment and is not conducive to learning - a provision which is central to the mission statement and ethos of St. Canice's School.

Internet Acceptable Usage (Pupils)

Educationalists believe in the benefits of curriculum-based internet use. The purpose of the Internet Acceptable Usage Policy is to ensure that pupils will benefit from learning opportunities offered by the school's internet resources, and will be protected from harmful and illegal use of the Internet.

St. Canice's School will employ a number of strategies to maximise learning opportunities and reduce risks associated with the Internet.

These strategies are as follows:

1. Internet Acceptable Usage Policy
2. Education
3. Filtering/Monitoring

Sanctions

If a pupil deliberately misuses the internet or email, this will result in disciplinary action, including the withdrawal of access privileges. Parents/guardians will receive written notification of misuse by a pupil.

Internet

1. Internet will be used for educational purposes only
2. Internet sessions will always be supervised by a teacher
3. Pupils will seek permission before entering any Internet site, unless previously approved by a teacher
4. Filtering software will be used to minimise the risk of exposure to inappropriate material
5. The school will regularly monitor pupils' internet usage
6. Pupils will receive training in the area of internet safety
7. Pupils will be taught to evaluate the content of internet sites
8. Teachers will be made aware of internet safety issues
9. Uploading and downloading of non-approved material is prohibited
10. Virus protection software will be used and updated on a regular basis

11. The use of personal disks, external storage devices or CD-ROMS in school requires a teacher's permission
12. Pupils will observe good "netiquette" (etiquette on the internet) at all times and will not undertake any action that may bring a school into disrepute
13. 'YouTube' (and similar sites) can be accessed only under the supervision and direction of the teacher.
- 14. St Canice's urge parents not to allow unsupervised access to the Internet at home.**
- 15. St Canice's recommends not allowing children access to digital devices in their bedrooms or unsupervised areas**
16. St Canice's will, from time to time organise meetings for parents on Internet Safety.

Email

If pupils are allowed to use email, the following rules will apply:

1. Email will be used for educational purposes only
2. Students will only use approved class email accounts under supervision by or permission from a teacher
3. Pupils will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person
4. Pupils will not send messages to or from school email
5. Pupils will not reveal their own or other people's personal details e.g. addresses, telephone numbers, or pictures via school email
6. Pupils will never arrange to meet someone via school email
7. Sending or receiving email attachments is subject to teacher permission.

Internet Chat

Students are not permitted to use internet chat rooms.

School Website (when built)

Designated teachers will manage the publication of material on the school website.

1. Personal pupil information, home addresses and contact details will not be published on the school website
2. Class lists will not be published

3. Pupils' full names will not be published beside their photograph
4. Digital photographs, video clips and audio clips will focus on groups and group activities rather than on individual pupils
5. Pupils will be given an opportunity to publish projects, artwork or school work on the school website
6. Teachers will select work to be published and decide on the appropriateness of such
7. Permission to publish a student's work will be sought from pupils/ parents/ guardians. This permission may be withdrawn at any time.
8. Pupils will continue to own the copyright on any work published.

Internal School Procedures:

The following are the guidelines for mobile phone/electronic games usage in the school;

- Children are not allowed to use mobile phones/electronic games during school hours
- Pupils are not allowed to bring mobile phones or electronic games into school. In exceptional circumstances, such as when out of school activities and after school games are scheduled, school tours etc., children may be allowed carry a phone as parents may need to be contacted this must be following prior consultation with the principal.
- Children who need to contact home during school hours may do so through the school secretary using the school landline phone
- All electronic gadgets are prohibited, even during after school activities
- Any pupil who brings a mobile phone or electronic game to school risks having it confiscated and not returned until the school day is over or to their parent/guardian.
- Staff have access to the school landline if urgent calls need to be made to parents
- Classroom supervision is usually organised if a class teacher has to contact other professionals or outside agencies in relation to a particular child
- Staff personal calls are normally confined to break times
- Staff are permitted mobile phone usage only in cases of emergency

Education

St. Canice's School will undertake an education programme to educate children on the safe, responsible use of the Internet.

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they need to learn to recognise and avoid these risks – to become internet wise.

Resources that may be used to implement this programme include

- NCTE Internet Safety Awareness Video
- Use of the 'Kids' section on the www.webwise.ie website
- SAFT Internet Safety Awareness Education Programme and exemplars

Filtering

'Filtering' is a term used to describe a way of limiting the content of web pages, emails, chat rooms and other electronic data to which users may be exposed. No filter is 100% accurate. The most effective filtering tool is adult vigilance.

Many browsers have their own built in filtering tool e.g. Google. Google's search engine has a built-in "Safe Search". This filter eliminates sites that contain pornography and explicit sexual content from search results. It is easily applied by clicking on the **Preferences** link on any Google page. Unfortunately it is also easily removed.

St. Canice's School has filtering software. The access to websites from all school computers is monitored and regularly reviewed by the NCCA. Websites are only allowed through following a verification of their suitability.

Firewalls

Windows XP has a built-in firewall. Firewall software can be purchased or downloaded free from the Internet. St. Canice's School has installed firewall software.

Legislation

There is a number of legislations that have relevance to Internet safety. Teachers, pupils and parents should familiarise themselves with them. They are briefly described as follows:

1. Child Trafficking and Pornography Bill 1998.

This Act legislates against anyone who knowingly produces, prints, publishes, distributes, exports, imports shows, possesses or sells child pornography.
<http://www.irlgov.ie/bills/1997/7397/default.htm>

2. 1993 Interception Act.

(The Interception of Postal Packets and Telecommunications Messages Regulation Act 1993). This Act stipulates that telecommunication messages can be intercepted for the purpose of an investigation of a serious offence. Authorisations are subject to certain conditions.

<http://193.120.124.98/ZZA22Y1989.html>

3. Video Recordings Act 1989.

The 1989 Video Recordings Act prohibits the distribution of videos, which contain obscene or indecent material, which may lead to the depravation, or corruption of the viewer.

<http://193.120.124.98/ZZA22Y1989.html>

4. The Data Protection Act 1988.

This Act was passed in order to deal with privacy issues arising from the increasing amount of information kept on computer about individuals.

<http://193.120.124.98/ZZA25Y1988.html>

Support Structures

The following are key support structures and organisation that deal with illegal material or harmful use of the Internet:

National Centre for Technology in Education

(<http://www.ncte.ie/internetsafety>) Provides information and advice on Internet safety issues for teachers and parents.

Hotline (<http://www.hotline.ie>)

Irish hotline for reporting online child pornography. Reports can be made by emailing report@hotline.ie or phoning 1890-610710.

Internet Service Providers Association of Ireland (<http://www.ispai.ie>)

An organisation that represents the Internet Service Providers' industry at national, European and international level.

An Garda Siochana (<http://www.garda.ie>)

IAB (Internet Advisory Board) (<http://www.iab.ie>)

An organisation that monitors developments regarding illegal and harmful use of the Internet.

Safer Internet Action Plan (<http://www.saferinternet.org>)

The Safer Internet Action Plan is the European Union's response to promoting safety on the Internet, addressing the controversial issue of illegal, harmful and racist content.

Barnados (<http://www.barnados.ie>)

Barnados is a leading independent agency for children and families.

COPINE (http://copine.ucc.ie/conf_main.php3)

The COPINE project is an initiative, which addresses the issue of child exploitation via the Internet.

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

Monitor, review and evaluation

This policy will be monitored, reviewed and evaluated on an ongoing basis in light of changing information, legislation, implementation issues, etc.

Communication

The ratified policy will be circulated to all parents and will be communicated to other members of the school community as appropriate.

Implementation Date

This policy will apply from the date of ratification by the Board of Management.

Ratification

This policy was read, discussed and approved/ratified by the Board of Management. Copies of the policy are available from the principal.

Signed: _____

Dated:

Marguerite Ahearne

Letter to Parents

Dear Parent/Guardian,

As part of the school's education programme we offer pupils supervised access to the Internet. This will allow pupils vast educational opportunities by helping them for example to locate material for projects, communicate with students from different cultures, become independent in controlling their own research and become independent learners.

While we as educationalists recognise the value of the Internet as a resource, we must also acknowledge the potential risks to students. We feel that the answer is not to ban the use of the Internet in school but to teach pupils to recognise the risks and to become **Internet Wise**. We also allow limited access to 'YouTube' on a strictly supervised basis. This is to allow access to a huge range of educational material. The filter to prevent access to unsuitable material on YouTube is also in operation.

This process is the responsibility of the school and the parent/guardian.

For this reason we have compiled a school policy on Internet safety and Digital Device Safety. Parents must also set and convey standards of usage to their children.

It is important that you read the school's Internet Policy and sign the attached document.

Parents should discuss this document with their children to ensure that they clearly understand the school rules with regard to Internet usage and Digital Device Safety. Please also get your child/ren (2nd – 6th class) to sign the attached document.

Mise le meas,

Principal

Internet Permission Form

Name of Pupil(s): _____

Class(es): _____

As the parent or legal guardian of the above child(ren), I have read the Internet Acceptable

Use Policy and grant permission for _____
(name(s): son/daughter) to access the Internet. I understand that school internet usage is for educational purposes only and that every reasonable precaution will be taken by the school to provide for online safety.

I accept my own responsibility for the education of my child(ren) on issues of Internet Responsibility and Safety.

I understand that having adhered to all the enclosed precautions the school cannot be held responsible if my child tries to access unsuitable material.

Signature: 1. _____ 2. _____

Parents/Legal Guardians

Date: _____

Pupil 1. _____ 2. _____

3. _____ 4. _____

.....
School Website

I understand that, if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the school's website. I understand and accept the terms of the Acceptable Usage Policy in relation to publishing pupils' work and photographs of school activities on the website.

Signature: 1. _____ 2. _____

Parents/Legal Guardians

Date: _____