

Meánscoil Iognáid Rís,
Nás na Rí
Co. Chill Dara.



Tel: (045) 866400
Fax: (045) 881580
Email: admin@naascbs.ie
Web: www.naascbs.ie

Principal: Mr. B. Travers
Deputy Principals: Ms. A. Meade
Mr. L. Murphy
Ms. S. Power

(AUP) ACCEPTABLE USAGE POLICY – May 2018

School Name: Meánscoil Iognáid Rís

School Address: Corban's Lane, Naas

School Details: Meánscoil Iognáid Rís is an all-boys Catholic voluntary secondary school under the Trusteeship of the *Edmund Rice Schools Trust*, formerly the Irish Christian Brothers. The school is named after the founder of the Order, Edmund Rice.

School Mangement: The Board of Management of Meánscoil Iognáid Rís is a statutory Board appointed pursuant to the provisions of the Education Act 1998.

MISSION STATEMENT

Inspired by its founder, Meánscoil Iognáid Rís aims to provide Catholic education in the Edmund Rice tradition. The school endeavours to be a caring Christian Community which promotes to the best of its ability the personal, spiritual, physical and intellectual development of its students

ETHOS

As an Edmund Rice School, Meánscoil Iognáid Rís seeks to promote the five key elements of an Edmund Rice School as espoused by the ERST Charter:

- Nurturing faith, Christian spirituality and Gospel-based values
- Promoting partnership in the school community
- Excelling in teaching and learning
- Creating a caring school community
- Inspiring transformational leadership.

Rationale:

The aim of this Acceptable Usage Policy (AUP) is to ensure that students will benefit from learning opportunities offered by the school's ICT and internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. If the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions will be imposed. It is envisaged that school and parent representatives will be involved in the review of this policy on a regular basis.

School's Strategy

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

- Internet sessions will always be supervised by a teacher
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material
- The school will regularly monitor students' internet usage
- Students and teachers will be provided with training in the area of Internet safety
- Uploading and downloading of non-approved software will not be permitted
- Virus protection software will be used and updated on a regular basis
- The use of personal memory sticks or other digital storage media in school, requires a teacher's permission
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute (see student digital citizenship document)

World Wide Web

- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials
- Students will report accidental accessing of inappropriate materials in accordance with school procedures
- Students will use the Internet for educational purposes only
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement)
- Students will never disclose or publicise personal information
- Downloading by students of materials or images not relevant to their studies is in direct breach of the school's acceptable use policy
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons

Email

- Students will use approved class email accounts under supervision by or permission from a teacher
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures
- Students will never arrange a face-to-face meeting with someone they only know through emails or the internet
- Students will note that sending and receiving email attachments is subject to permission from their teacher

Personal Devices

Students using their own mobile devices in school should follow the rules set out in this agreement. They will only use personal hand held / external devices (mobile phones / USB devices etc) in school if they have permission.

Support Structures


The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of 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.

School Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit and risks/disadvantages of using these technologies for education:

 Communication Technologies	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✗			
Use of mobile phones in lessons			✗	
Use of mobile phones between lessons/outside classrooms				✗
Use of mobile phones in social time		✗		
Taking photos on mobile phones or other camera devices				✗
Use of hand held devices e.g. PSPs				✗
Use of personal email addresses in school, or on school network				✗
Use of school email for personal emails				✗
Use of chat rooms / facilities				✗
Use of instant messaging				✗
Use of social networking sites				✗
Use of blogs			✗	

Cyberbullying - Understanding Cyber Bullying:

- Cyber bullying is the use of ICT (usually a mobile phone and/or the internet) to abuse another person.
- It can take place anywhere and can involve many people.
- Anybody can be targeted, including pupils, school staff, and members of the wider school community.
- It can include threats, intimidation, harassment, cyber-stalking, vilification, defamation, exclusion, peer rejection, impersonation, and unauthorised publication of private information or images.

There are many types of cyber-bullying. The more common types are:

1. **Text messages** – can be threatening or cause discomfort. Also included here is ‘Bluejacking’ (the sending of anonymous text messages over short distances using Bluetooth wireless technology)
2. **Picture/video-clips via mobile phone cameras** – images sent to others to make the victim feel threatened or embarrassed.
3. **Mobile phone calls** – silent calls, abusive messages or stealing the victim’s phone and using it to harass others, to make them believe the victim is responsible.
4. **Emails** – threatening or bullying emails, often sent using a pseudonym or somebody else’s name.
5. **Chat room bullying** – menacing or upsetting responses to children or young people when they are in a web-based chat room.
6. **Instant messaging (IM)** – unpleasant messages sent while children conduct real-time conversations online using MSM (Microsoft Messenger), Yahoo Chat or similar tools.
7. **Bullying via websites** – use of defamatory blogs (web logs), personal websites, gaming websites, and online personal ‘own web space’ sites such as You Tube, Facebook, Ask.fm, Instagram, Twitter, SnapChat, and Myspace, among others.

Procedures for preventing Cyber Bullying:

1. Staff, pupils, parents, and Board of Management (BOM) are made aware of issues surrounding cyber bullying.
2. Pupils and parents will be urged to report all incidents of cyber bullying to the school.
3. Staff CDP (Continuous Professional Development) will assist in learning about current technologies.
4. Pupils will learn about cyber bullying through Social, Personal and Health Education (SPHE), Assemblies and other curriculum projects.
5. Pupils, parents, and staff will be involved in reviewing and revising this policy as school procedure.
6. All reports of cyber-bullying will be noted and investigated, in accordance with the school’s Anti-Bullying, Mobile Phone, Child Protection, and Positive Behaviour Policies, where applicable.
7. The school will engage a speaker Community Guard to facilitate a workshop on Internet Safety and mark Safer Internet Day (SID) annually.
8. Procedures in the school’s Anti-Bullying and Child Protection policies shall apply.

Incidents of cyberbullying will be addressed in the following policies:

- Child Protection Guidelines
- Mobile Phone Policy
- Anti-Bullying Policy
- ICT Policy

Legislation

The school will make available, information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

- Data Protection Act 1988 (and Amendment Act 2003)
- <http://www.dataprotection.ie/>
- <http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html>
- <http://www.irishstatutebook.ie/2003/en/act/pub/0006/index.html>
- Child Trafficking and Pornography Act 1998
- <http://www.irishstatutebook.ie/1998/en/act/pub/0022/index.html>
- Interception Act 1993
- <http://www.irishstatutebook.ie/1993/en/act/pub/0010/print.html>
- Video Recordings Act 1989
- <http://www.irishstatutebook.ie/1989/en/act/pub/0022/index.html>

Support Structures

Where appropriate, the school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet. CBS Naas has adopted the Child Protection Procedures for Primary and Post Primary Schools as part of its child protection policy. This policy has been made available to the Parents' Council and is available to all parents on request.

DESIGNATED LIAISON PERSON (DLP)

Ben Travers (Principal)

DEPUTY DESIGNATED LIAISON PERSON (DDLDP)

Anne Meade (Deputy Principal)



Naas CBS Safe Internet Usage Policy

This policy is informed by the vision for Naas CBS coupled with the school's ethos which aims to enable students to reach their full potential both academically and socially.

Respect Yourself

I will show respect for myself through my actions. I will only use appropriate language and images on the Internet or on the school website / virtual learning environment. I will not post inappropriate personal information about my life, experiences or relationships.

Protect Yourself

I will ensure that the information I post online will not put me at risk. I will not publish full contact details, a schedule of my activities or inappropriate personal details in public spaces. I will report any aggressive or inappropriate behaviour directed at me. I will not share my password or account details with anyone else.

Respect Others

I will show respect to others. I will not use electronic mediums to bully, harass or stalk other people. I will not visit sites that are degrading, pornographic, racist or that the school would deem inappropriate. I will not abuse my access privileges and I will not enter other people's private spaces or work areas. I will respect my peers and teachers by not using technology inappropriately in or out of class.

Protect Others

I will protect others by reporting abuse. I will not forward any materials (including emails and images) that the school would deem inappropriate.

Respect Copyright

I will use and abide by the fair use rules. I will not install software on school machines without permission. I will not steal music or other media, and will refrain from distributing these in a manner that violates their licenses.

Respecting Technology

I will take all reasonable precautions to protect my mobile device from damage. I will always keep it with me or in secure storage when appropriate.

Acceptance

By signing this agreement, I agree to always act in a manner that is respectful to myself and others, in a way that will represent the school in a positive way. I accept that this policy applies in school and outside school. I understand that failing to follow the above will lead to appropriate sanctions being carried out.

Student

Parent/Guardian

Date