St. Mary's College
Preparatory School

Network and Internet Use Policy for Pupils

Date Written: August 2016
Reviewed September 2024

St Mary's College Preparatory School – The Prep

Network and Internet Use Policy for Pupils
(This policy includes EYFS Reception, KS1 and KS2)

This policy has been written in consultation with staff and governors of the Prep and with due regard to the school's mission statement:

Our Mission is to provide an independent Catholic education for boys and girls of all faiths aged 0-18; to provide individual challenge towards holistic and balanced development, service and achievement for life and beyond; and to try to show our Faith by the way we live, showing care and consideration for each other, those around us and the environment.

1. Student access to the Internet

The Prep encourages use by students of the rich information resources available on the Internet, together with the development of appropriate skills to analyse and evaluate such resources. These skills will be fundamental in the society our students will enter.

On-line services significantly alter the information landscape for schools by opening classrooms to a broader array of resources. In the past, teaching and library materials could usually be carefully chosen. All such materials will be chosen to be consistent with national policies, supporting and enriching the curriculum while taking into account the varied teaching needs, learning styles, abilities and developmental levels of the students. Internet access, because it may lead to any publicly available site in the world, will open classrooms to electronic information resources which have not been selected by teachers as appropriate for use by students.

Electronic information research skills are now fundamental to preparation of citizens and future employees. The school expects that staff will begin to investigate possibilities and blend use of such information as appropriate within the curriculum and that staff will provide guidance and instruction to students in the appropriate use of such resources. Staff will consult the Headmaster or Head of ICT for advice on content, training and appropriate teaching levels consistent with the Prep's IT program of study.

Access to on-line resources will enable students to explore thousands of libraries, databases and bulletin boards including the use of e-mail. The school believes that the benefits to students from access to information resources and increased opportunities for collaboration exceed the disadvantages. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for independent access.

The purpose of this policy is to balance the desirability of staff and pupils being able to access the vast educational potential of new technology while, at the same time, providing safeguards against risks and unauthorised material and activities.

The College's Head of ICT has prepared appropriate procedures below for implementing this policy and for reviewing and evaluating its effect on teaching and learning.

2. Roles and Responsibilities

E-safety is primarily a safeguarding issue so anyone with responsibility for the welfare of children has responsibility for ensuring that information is accessed safely. The College takes it's responsibilities under the DFE documents *'Keeping children safe in education, September 2023'* and *'The Prevent Duty, 2023'* seriously and this document should be referred to, along with consulting the Designated Person, if in any doubt. Pupils also have responsibilities and will be encouraged to develop their own sets of safe behaviours.

(a) Pupils

Responsibilities for pupils include:

- Contributing to the safety of e-safety policies
- Reading the rules – and adhering to them
- Taking responsibility for keeping themselves and others safe online
- Behaving safely and responsibly to limit the risks of Internet usage
- Respecting the feelings of others
- Reporting any abuses of the rules

(b) The School

The School is responsible for the effective management of safety of the Internet and for making appropriate resources available to support the development of a safe culture. Its role is delegated to the Headmaster. His responsibilities are to;

- develop a safety culture and to act as a point of contact on all e-safety issues
- ensure that all staff are trained in e-safety
- ensure that e-safety is embedded across the curriculum
- ensure that e-safety is promoted to parents in life outside the Prep
- prepare reports dealing with e-safety and review any breaches of safety
- review policies and procedures on a regular basis

(c) Parents

Parents also have responsibilities as follows:

- discussing e-safety with their children and reinforcing appropriate behaviours at home
- liaising with the Prep if they suspect or have identified that their child is conducting risky online behaviour

3. School Procedures

Resource Development

In order to match electronic resources as closely as possible to the Prep curriculum, teachers will review and evaluate resources in order to offer materials that are appropriate to the age range and

ability of the group being taught. Staff will provide appropriate guidance to students as they make use of telecommunications and electronic information resources to conduct research and other studies. All students will be informed by staff of their rights and responsibilities as users, before their first use, either as an individual user or as a member of a class or group.

As far as possible, the School's chosen information provider has organised information resources in ways that point students to those that have been reviewed and evaluated prior to use. Whilst students may be able to move beyond these resources to others that have not been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. Students may pursue electronic research independent of staff supervision only if they have been granted parental permission and have submitted all required forms. Permission is not transferrable and may not be shared.

School Rules
The school has developed a set of guidelines for Internet use by students. These rules will be made available to all students, and kept under constant review.

All members of staff are responsible for explaining the rules and their implications. All members of staff are aware of possible misuses of on-line access and their responsibilities to all students.

4. Acceptable User Policy for all users of the school network

Access to the school network will be provided for you to carry out recognised school work, but only on the understanding that you agree to follow these guidelines.

Computer (file) storage areas will be treated as school property. ICT staff may look at files and communications to ensure that the system is being used responsibly. Users should not expect that their work and emails would always be private.

The following are not permitted: -

- Sending or displaying offensive messages or pictures.
- Using obscene language.
- Harassing, insulting or attacking others.
- Damaging computers, computer systems or computer networks.
- Violating copyright laws.
- Using others' passwords.
- Trespassing in others' folders, work or files.
- Intentionally wasting limited resources.
- Accessing terrorist and/or extremist material whilst on the internet in College.

- Users are responsible for good behaviour on the network just as they are in a classroom or at school. General school rules apply.

- Eating, drinking, personal grooming, and the use of aerosol sprays are not considered to be suitable activities in any classroom. Near a computer they may cause serious damage and are strictly prohibited.

- Please do not spend too long sending/receiving e-mail messages – someone else is usually waiting to use the computer. You should not waste valuable resource time sending trivial e-mails to another person in the College, or to anyone else for that matter.

- Important work files should be copied to a personal USB stick or saved to the cloud with Microsoft OneDrive in case you accidentally damage them or delete them from the network service.

- If a "virus alert" occurs when using a USB stick, please inform a member of staff immediately and do not use until it has been verified as safe.

- Do not use another person's password. If doing shared work, you must keep a copy of the work on your own disk in case your partner is absent from school.

- Do not reveal your password to anyone. If you think someone has learned your password then change it immediately.

- Change your password at regular intervals; at least once a term using a minimum of six characters.

- Do not trespass in others' folders, work or files.

- The unauthorised access or use of personal information, contrary to the provisions of the Data Protection Act 2018, is not permitted.

- Intentional damage to computers, computer systems or computer networks, including unauthorised damage or interference to any files is not permitted and may be considered a criminal offence under the Computer Misuse Act 1990.

- Programs must not be installed on a computer except by a qualified technician. Do not bring in programs on a disk or download them from the Internet.

- Games must not be loaded, played or used on any computer unless used for authorised training or teaching purposes.

- The unauthorised copying of software, contrary to the provisions of the Copyright, Design and Patents Act 1988 is not permitted.

- The installing, copying or transmitting of obscene material is not permitted and may be considered a criminal offence under the Obscene Publications Act 1959/1964.

- A computer should not be switched off during the school day unless it has completely locked up or is unlikely to be used again that day.

- Always make sure that you have completely logged off the computer before leaving it unattended.

- Please leave the computer and the surrounding areas as you find them.

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on your use of the school network.

2. Additional disciplinary action may be added within line of existing practice on inappropriate language or behaviour.

3. When applicable, police or local authorities may be involved.

This policy will be communicated to all users and will be reviewed at least annually by the Headmaster and Network Manager.