St Richard's Catholic College

ACCEPTABLE USE POLICY

(from School Handbook)

The Policy was approved by the Governing Body: June 2022

Chair of Governors: _____

The Governing Body will review the policy in June 2023

Acceptable Use Policy

'Acceptable and Responsible Use of ICT Resources'

The benefits of Internet Access for Education

Access to the Internet offers both pupils and staff vast, diverse, and unique resources. The Internet opens up opportunities to initiate cultural exchanges between pupils from all over the world, whilst at the same time providing access to educational, social and leisure resources.

The main reason that we provide Internet access to our staff and pupils is to promote educational excellence by facilitating resource sharing, innovation, and communication. However, for both pupils and teachers, **Internet and Email access at school are privileges and not an entitlement.**

a. Staff are responsible for guiding pupils in their online activities, by providing clear objectives for Internet use.
b. Staff will also ensure that pupils comply with this Acceptable Use Policy ("AUP") by reminding them of what is regarded as acceptable and responsible use of the Internet.
c. The use of internet games is strictly prohibited.
d. The use of USB storage is strictly prohibited

The main goal is to utilise Internet access to enrich and extend those learning activities that reflect the curriculum requirements and the age and maturity of the pupils.

All Internet access is filtered internally to screen out undesirable sites.

School Network Security Strategies

The school's computer network security systems are reviewed regularly. The school will regularly check user files, temporary Internet files, history files and internet access logs.

Our number one priority is to put the safety of the pupils' use of the internet first – with the recent implementation of the Online Safety policy used throughout the educational software.

Uploading, Downloading, Execution and Creation of non-approved application software is denied. Any evidence of unauthorised software being on school equipment will be reported to Pastoral Leaders, resulting in a *full access ban* for two weeks. All access to the school network requires entry of a recognised User ID and password. All pupils must lock their computer when leaving it unattended and they must log out after every session/class – or warrant being logged out by the ICT Services Team.

Virus protection software is installed and updated regularly on all Client and Server Based systems.

Unapproved system utilities software and executable files are not allowed to be stored in pupil storage areas.

Pupils *are not permitted* without direction from the Director of ICT Services to write or execute their own scripts.

Hardware and Software Infrastructures

The school has invested in the following hardware and software infrastructures to reduce risks associated with the Internet:

- Unified Threat Management Server and Firewall
- Client Server network – for the easy management of clients using the St Richard's Network.
- Network & client monitoring software – detects typed or on screen language, inappropriate internet content and pictures.
- Webpage filtering software to filter out inappropriate websites to study.
- Classroom Monitoring Software for ICT Suites – to allow the teacher to keep a close track on the movements of pupils while using ICT equipment.

Classroom Management Structures

Planned seating is to be used in all ICT suites to allow teachers to trace and monitor pupil access and usage of the Internet.

Pupils using ICT suites are to report any faulty equipment to the teacher leading the session.

Under no circumstance are pupils to attempt to repair any ICT hardware or software.

Risk Assessment and Management of Internet Content

The school has taken and will continue to take all reasonable precautions to ensure that pupils access appropriate material only. However, it is not possible to guarantee that a pupil will never come across unsuitable material while using a school networked computer. The school, however, cannot accept liability if such material is accessed nor for any consequences resulting from Internet access.

All pupils are taught effective online research techniques, including the use of subject catalogues and search engines. Receiving information over the web or in e-mail or text messages presupposes good information-handling skills.

Key online information-handling skills include:

- Ensuring the validity, currency and origins of the information accessed or received
- Using alternative sources of information for comparison purposes
- Identifying an author's name, date of revision of the materials, and possible other links to the site
- Respecting copyright and intellectual property rights

Pupils will be made fully aware of the risks to which they may be exposed while on the Internet. They will be shown how to recognise and avoid the negative areas of the Internet such as pornography, violence, racism and exploitation of children.

However, if they encounter such material, pupils must ensure that they switch off the monitor, not the computer, and report the incident to the nearest member of staff or

the school's ICT Services Team.

Regulation and Guidelines

The school's Internet access incorporates a software filtering system to block certain chat rooms, newsgroups, and inappropriate websites. The filtering system used on the school network aims to achieve the following:

- Access to inappropriate sites is blocked.
- The content of web pages or web searches is dynamically filtered for unsuitable words.
- A rating system is used to rate web pages for inappropriate content and the web browsers are set to reject these pages.
- Records of banned Internet sites visited by pupils and staff are logged.
- Accessing a site denied by the filtering system will result in a report being generated and sent to the Director of ICT Services for appropriate action.

The school will immediately report the details of any illegal Internet material found.

Similarly, staff will request that 'allow' access be made of certain banned sites and provide the educational reasons behind the request.

Email Accounts

Pupils should immediately report any offensive emails that they receive to the teacher leading the session.

Access in school to external, Web-based, personal email accounts is denied for network security reasons.

- It is forbidden to distribute chain letters or to forward a message without the prior permission of the sender.
- It is forbidden to send executable files via email.
- Pupils must read their emails regularly and remove superfluous emails from their mailbox.
- Pupils may not reveal their own or other people's personal details such as addresses or telephone numbers or arrange to meet someone outside school via the school network.
- Sending and receiving email attachments is subject to the type allowed by the school's filtering policy.
- Pupils must not use their school account to send out group or whole school emails.

The School Website

The ICT Services Team and Administration Team manages the school's website, which complies with the Local Authority's guidelines.

The copyright of all material produced by the school for display on the school's web pages belongs to the school. **Permission to reproduce any other material will be sought and obtained from the copyright owner.**

The contact details for the school will include only the school's postal address, e-mail address and telephone number. No information about staff's home addresses or the like will be published.

The school will not publish any material produced by pupils without the agreed permission of their parents/carers. In addition, photographs of pupils will not be published without a parent or carer's written permission. A pupil's full name will not be used in association with photographs.

Website photographs that include pupils will be carefully selected and will be of a type that does not allow individual pupils to be identified - group photographs or 'over the shoulder' images are preferred.

Moderated Mailing Lists, Newsgroups and Chat Rooms

The school uses an email distribution list to send messages to selected groups of users. Pupils are denied access to chat rooms inclusive of instant messaging services.

Other communication technologies

Pupils are not allowed to use mobile phones within the school building or classrooms. This clause covers other mobile devices containing similar functionality. It is forbidden to send abusive or otherwise inappropriate messages using the facilities provided by the school network.

Consequences

Pupils should note that the following abuse of the school network represents gross misuse and will lead to consequences and the possible loss of their account being imposed:

a. Allowing any other person to use or access their personal account. – Pupils will have their account immediately suspended for TWO WEEKS as this represents a serious breach of this policy
b. The inappropriate display of data of any teacher, pupil or staff member which breaches the requirements of the data protection act. **Pupils will have their account immediately suspended *until further investigation* as this represents a serious breach of this policy**
c. Less serious misuse will be, at the discretion of the ICT Services Team, governed by the use of a staircase system. Incidents classed under this category include but are not exclusive to:
    i. The use of games
    ii. Cyber bullying
    iii. Inappropriate use of email
d. The use of executable files, batch scripts or VB scripts on the network incurs a two week **full** ban. This includes general hacking exploitations.

No Logon Username, Password or E-mail Address will be issued without agreement of this policy.