# A SCHOOL ACCEPTABLE USE POLICY

An Acceptable Use Policy addresses all rights, privileges and responsibilities associated with the Internet. Ideally every school will devise an AUP before it is involved in any use of the Internet.

The following exemplar whole-school policy, which refers to the safe, acceptable and responsible use of the Internet, has been devised and can be used by other schools as a framework for creating an AUP. It is based on local and national guidelines and may be incorporated into the school's overall ICT policy.

It is envisaged that teachers, ICT co-ordinators, local education/municipality officers and parent associations will approve and contribute to this AUP. It is also intended that the policy will be reviewed annually and updated as required.

**All involved parties should read the AUP and its annexes carefully to ensure that they fully understand and accept the contents before signing it.**

---

## ST. ALPHONSUS R.C. PRIMARY SCHOOL

**'Acceptable and Responsible Use of ICT Resources'**

This version was created on March 2026 by Miss G Harrison

Approved by Governors

**Contents**

## 1 THE BENEFITS OF INTERNET ACCESS FOR EDUCATION

Most curricula at European level require students to demonstrate that they can effectively locate, retrieve and exchange information using ICT. Access to the Internet offers both students and teachers vast, diverse, and unique resources. The Internet opens up opportunities to initiate cultural exchanges between students from all over the world, while at the same time providing access to educational, social and leisure resources.

The main reason that we provide Internet access to our teachers and students is to promote educational excellence by facilitating resource sharing, innovation, and communication. However, for both students and teachers, Internet access at school is a privilege and not an entitlement.

Unfortunately as there is the possibility that students will encounter inappropriate material on the Internet, the school will actively take all reasonable precautions to restrict student access to both undesirable and illegal material.

Teachers are responsible for guiding students in their on-line activities, by providing clear objectives for Internet use. Teaching staff will also ensure that students are only too aware of what is regarded as acceptable and responsible use of the Internet. 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 students.

Students will access websites from bookmarks within the 'Favourites' folder in their browser. These will have been previewed and approved by their teacher.

The free use of search engines is permitted only when another teacher or member of staff is present. Child friendly search engines, for example yahooligans.com and Google Safe Search can filter most websites with inappropriate content and will be used as a first option. Other search engines intended for use by students offer a filtered list of links.

All Internet access is filtered through a proxy server to screen out undesirable sites at source

## 2 WHOLE-SCHOOL NETWORK SECURITY STRATEGIES

The school's computer network security systems are reviewed at least once per week by the ICT technicians.

The school will check user files, temporary Internet files and history files once a week.

Uploading and downloading of non-approved application software is denied.

All access to the school network requires entry of a recognised User ID and password. Students must log out after every network session.

Virus protection software is installed and updated regularly by ICT technicians.

Using personal memory cards on the school network requires specific teacher permission and a virus check.

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

ICT technicians check student files held on the school's network regularly.

**Hardware and software infrastructures**

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

Proxy server – in conjunction with a web management system

Filtering software

Firewall – that has been configured to prevent access to inappropriate websites.

**Classroom management structures**

Planned seating will allow teachers to trace and monitor student access and usage of the Internet.

Ensure that computers are positioned in such a way that monitors are easily observed by teachers.

## 3 RISK ASSESSMENT AND MANAGEMENT OF INTERNET CONTENT

The school has taken and will continue to take all reasonable precautions to ensure that students access appropriate material only. However, it is not possible to guarantee that a student 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 students 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.

Students 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 they will know that they should switch off the monitor, not the computer, and report the incident to the nearest teacher or the school's ICT co-ordinator who will deal with it according to the school AUP.

## 4 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 that the web browsers are set to reject these pages.
- Records of banned Internet sites visited by students and teachers are logged.

Accessing a site denied by the filtering system will result in a report being generated and sent to the school's ICT Co-ordinator for appropriate action.

The school's ICT Co-ordinator regularly assesses the effectiveness of the filtering system. The school's filtering strategy depends on the age and curriculum requirements of each class.

In line with KCSiE 2025 it is essential that children are safeguarded from potentially harmful and inappropriate online material. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk: content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing

of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and commerce:
Risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel our pupils, students or staff have been exposed we will report it to the Anti-Phishing Working Group (https://apwg.org/).
The Governing body will ensure online safety is a running and interrelated theme in collaboration with our safeguarding policies and procedures.

The school will immediately report the details of any inappropriate or illegal Internet material found to Miss G Harrison.

### 4.1 E-mail accounts

Students may only use their approved e-mail account/s on the school network during school time.

Students shall immediately report any offensive e-mails that they receive to Miss G Harrison.

E-mail addresses are created for a whole class or teaching groups, not for individuals.

Access in school to external, Web-based, personal e-mail 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.

Students must read their e-mails regularly and remove superfluous e-mails from the server.

Students may send spam messages only if they are required to do so as part of, for example, project work. Permission from the teacher will always be required to do this.

Students 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 e-mail attachments is subject to permission from the teacher.

.

### 4.2 Moderated mailing lists, newsgroups and chat rooms

The school may use/uses an e-mail distribution list to send messages to selected groups of users.

Teachers will moderate other collaboration tools such as newsgroups and chat rooms if used on the school network for learning purposes.

Students will be denied access to public or unmoderated chat rooms.

Only regulated educational chat environments shall be used. They will always be used under supervision. Safety is the major consideration.

Only newsgroups that have educational goals and content will be made available to students.

### 4.3 Other communication technologies

Students are not allowed to use mobile devices during lessons or formal school time. It is forbidden to send abusive or otherwise inappropriate text messages using the facilities provided by the school network.

## 5 COMMUNICATING THE SCHOOL'S AUP

### 5.1 Informing students

'Code of Practice' posters will be displayed near all networked computer systems. Students will be informed that their Internet use is monitored and be given instructions on safe and responsible use of the Internet. The school has created separate Rules for Acceptable and Responsible Internet Use for primary and post-primary grades, if appropriate.

### 5.2 Informing staff

All staff will be provided with a copy of the School's Acceptable Use Policy. Staff will be consulted regularly about the development of the school's Acceptable Use Policy and instructions on safe and responsible Internet.

To avoid misunderstandings teachers will contact the ICT Co-ordinator regarding any doubts that arise concerning the legitimacy of any given instance of Internet use. Teachers will be provided with information on 'copyright and the Internet' issues that apply to schools.

### 5.3 Informing parents / carers

Parents' attention will be drawn to the School AUP by letter. Advice that accords with acceptable and responsible Internet use by students at home will be made available to parents. Safety issues will be handled sensitively.

The school will obtain parental consent before publication of students' work or photographs.

All comments on and suggestions concerning this Acceptable Use Policy should be sent to:

Miss G Harrison