I.T. ACCEPTABLE USE POLICY FOR STUDENTS

St John's Catholic Comprehensive School

Excellence for All
Service to Others
Inspired by Christ

Date of last review:	May 2025	**Date of next review:**	May 2026
Owner:	Data Protection Officer	**Quality Assures:**	Associate Headteacher
Approval:	Full Governing Body Panel		

Computing devices in the school and their use

All cabinets and trolleys are assigned to departments and should not be shared or moved without express permission of the Department Leader. The School's specialist IT rooms and desktop devices must be treated with due care at all times.

We ask students at St John's to be responsible for the following areas:

- To respect our I.T. Resources by looking after them and ensuring they are returned in the same state as when you found them.
- To report any damage to a member of teaching or support staff.
- Sixth form students are not permitted to use school devices in the café area but may use school devices in their study area.
- If you use a mobile device, return it back to the cabinet from where it came and ensure that it is placed back on charge.

St John's provides access to networked devices to support students' academic work. Our Acceptable Use Policy (AUP) is an extension to the Code of Practice provided by the General Teaching Council. It includes guidelines for the safe and responsible use of the network, e-mail and Internet, and identifies those activities which constitute a direct violation of our rules for our I.T. facilities. **Failure to comply with any aspect of our AUP could result in sanctions, bad comments or in serious cases be referred to your head of year or the child protection officer.**

Using our computer network

- The school I.T. systems may not be used for private purposes unless the Head Teacher has given specific permission.
- School device access must be made via your authorised school account and password which has been provided by technical support during your admission. Your login details must not be shared with any other person.
- All network and Internet use must be appropriate to education and this use is monitored by the technical support team.
- Using the school systems for personal financial gain, gambling, political activity, advertising or anything that can be considered against the law of the United Kingdom and could lead to both reporting and prosecution; dependent on the severity of the incident.
- Any use of the network that would bring the name of the school into disrepute is not allowed and could invoke a sanction. This includes the use of email and social media.
- Any use of the school network for plagiarising of students' work is forbidden; copying or plagiarising of examination coursework could lead to a student being disqualified from **ALL examinations in all subjects**. If a student is concerned that their work has been copied, they should immediately inform the school's exams officer.

Using our email systems and the internet

- We provide both email and internet services at the school and make use of various web-based technologies, everyone's access is monitored by an automated system that checks for any breach of this acceptable use policy.
- At all times copyright and intellectual property rights must be respected, if in doubt of whether something is copyrighted, and you would like advice please contact a member of technical support or your teacher.
- Blanket e-mails should not be sent to all students. Students **should not "reply to all"** if the message is **only intended for the sender.**
- As with any correspondence, messages should be written carefully and politely, particularly as an email could be forwarded to unintended readers or given to parents of other students at the school. Any email sent that brings the name of the school into disrepute could invoke a sanction.
- Anonymous messages and chain letters are not permitted at the school. If you are added to a mailing list that you wish to be removed from, contact technical support for assistance.
- Should a student be in receipt of any phishing emails, or messages from suspicious sources, they are to inform their teacher or a member of technical support at the earliest opportunity.
- The e-mail system must not be used to intimidate, bully or otherwise threaten another person(s) regardless of whether they are a St John's student, staff member or from outside of the school.
- Students should only use the school e-mail account when communicating electronically with staff. The use of external email services for work to be sent to or from is forbidden for both your own and the staff member's protection. Should you have any queries around what can be sent via email please contact the technical support team or a member of teaching or support staff.
- The email system is the property of the school, and the school has the right to view any email contained within the system at any time. This is always monitored automatically by the school's protective systems.
- Should you be aware of a successful attempt by a student to access a forbidden site containing pornographic images or other illicit material you must inform your teacher or a member of the technical support immediately so that we can ensure the site is blocked as soon as possible.

Social Media Use

- Staff members will not accept students as members of their social networking sites, unless it is a school account that has been specifically set up for this purpose.
- Any item posted by a student of the school on any public internet site such as a Website, Twitter or Facebook must be endorsed to that effect. The school's social media policy does not infringe your right to privacy but public forums could be monitored. If you have any concerns regarding the use of public forums, please speak to a member of teaching or support staff.
- As per the Domestic Violence Act, abusive behaviour by students or staff to partners on social media sites can now be prosecuted as a criminal offence. Should the school be made aware of any such incidents and/or evidence, the school will be duty bound to inform the police of any concern.
- As part of the anti-radicalisation "Prevent" strategy the school will actively monitor where possible and report on any findings that relate to extremism, should any such concern exist the school has a duty of care to pursue and inform the police of any concern.

Our monitoring systems

The school currently uses an automated monitoring system known as “Impero”. This system allows school staff members to monitor the laptop screens in lessons. The system is multi-faceted and allows instant detection of key words and hidden scripts and in addition photographic material of concern in any program that relate to any of the aforementioned areas of concern. All staff members are also monitored by this system. Should an issue arise, screenshots are automatically taken known as “violations” and forwarded to the technical support team members for analysis and if required passed to our school’s child protection officer.

Media Publications – What happens with photos taken in your lesson?

- Images of students (e.g. photographs, videos, web broadcasting, TV presentations, web pages etc.) must not be published under any circumstances unless authorised by a member of school leadership.
- Written permission from parents or carers needs to be obtained before photographs of students are published on the school website, including photographs in the newsletter. When joining the school, a photo release form will be given to your parents/carers as part of your school welcome pack. The school office has a list of names of students whose parents have not given written permission; staff must check with the school office before including any photographs in newsletters or on the school website.
- Students’ work will only be published (photographs, videos, TV presentations, web pages etc.) if parental consent has been given (note that this does not include photographs taken as part of school marketing).
- Students’ work, completed for school should not appear on any websites e.g. Facebook. Photographs taken in school should not appear on such websites.
- Use of the schools OneDrive accounts and other software accessed from home via the Internet should be treated with the same due regard for safeguarding privacy and confidentiality of students and staff and their work.