I.T. ACCEPTABLE USE POLICY FOR STAFF

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		

Support Team Services

The school runs an in-house support service for any computer based issue. All queries and problems related to technical issues should be reported in person to the help desk or via email to **technical@stj.kent.sch.uk**. Additionally, issues can be reported to Technical Support via phone communication; the extension for the Technical office being **5009**. Problems or queries will be responded to on the same day. **Technical support hours are from 8am until 4pm**. Calls logged after 3.30pm will be assigned for the following day unless critical to the next working day.

Computing devices in the school and their use.

All cabinets and trolleys are to departments and should not be shared or moved without seeking permission from the respective Subject Leader.

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

- To provide clear guidance and instruction to students in caring for devices; ensuring they are treated with respect and returned to storage sensibly and put back on charge.
- Work with your Subject Leader(s) to ensure the department systems for booking and return of laptop trolleys is adhered to.
- To report any laptop damage to technical via the help desk or email. Precise information should be given where possible i.e., the name of the cabinet, as well as the asset tag of the device. This is found on the device security label.
- Sixth form students are not permitted to use school devices in the café area but may use school devices in their study area. Please be vigilant to ensure devices are used in an appropriate area.
- To respect the devices that you are assigned and ensure they are kept safe, please ensure your staff device is covered by your home insurance policy if you intend to take it home.

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. It 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 be referred to your line manager for disciplinary action.**

Using our computer network

- The school I.T. systems may not be used for private purposes, unless the Head Teacher has given specific permission, for example inviting visitors to use the IT systems without prior permission.
- At all times it is expected that computer access and use must be made via your authorised school account and password. This is provided by technical support during your induction. You must not share your login details with any other person.
- All network and internet use must be appropriate to education. Your network and internet use is monitored by the technical support team.
- Using the systems for personal financial gain, gambling, political activity, advertising or anything that can be considered against the law of the United Kingdom 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 be considered a disciplinary matter. This includes the inappropriate 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**; staff must report any breach of this policy to the school's exam 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. All 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 you are in doubt as to whether something is copyrighted and you would like advice, please contact a member of technical support or the content provider.
- Blanket e-mails should not be sent to all staff unless related to an event or request relating to the running of the school or activities within it. Staff **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 emails could be forwarded to unintended readers or given to parents of students at the school. Any email sent that brings the name of the school into disrepute could lead to disciplinary action.
- 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, please contact technical support for assistance.
- The e-mail system must not be used to intimidate, bully or otherwise threaten another person(s) regardless of whether they are a member of St John's School staff or not.
- If you are in receipt of any suspicious emails or phishing messages, please inform Technical support as soon as possible.
- Staff should only use their school e-mail account when communicating electronically with students. The use of external email services for sending or receiving work related information / documents is forbidden for the protection of both staff member(s) and student(s). Should you have any queries regarding what information/documentation can be sent via your school email address, please seek guidance from a member of the technical team.
- 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. It 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 technical support immediately so that we can ensure the site is blocked as soon as possible.

Social Media Use

- Staff members should not accept students as members of their social networking sites. Staff members who wish to use any form of social media to interact with students must contact one of the school's Designated Safeguarding Leads (DSL) for advice and express written permission. In the instance of a staff member having a student at the school already connected to their social media through an existing relationship, they are required to make the Head Teacher and one of the school's Designated Safeguarding Leads aware of this at the very earliest opportunity.
- Any item posted by a staff member 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 use of public forums, please discuss with your line manager and one of the school's DSL.
- 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 and report 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 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.

Physical Security

Staff users are expected to ensure that portable IT equipment such as laptops, netbooks, digital still and video cameras are securely locked away when they are not being used. All mobile devices must be checked before use and placed back in their trolleys at the end of the lesson.

Departments will be held responsible for damage of devices if not reported to the helpdesk as soon as identified.

Media Publications

- Images of students (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 un-named photographs of students are published on the school website, including photographs in the newsletter. 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.
- 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 their work.