ACCEPTABLE USE POLICY

STUDENTS AND STUDENTS' VISITORS

MAY 2023

Acceptable Use Policy
Students and Student Visitors
Last Update Status: May 2023

What is an Acceptable Use Policy?

An acceptable use policy, also known as an AUP, is an agreement that outlines the appropriate use of access to a school's network, computer systems and data by detailing what users may or may not do when utilizing these platforms, including online and offline. The acceptable use policy sets out what we accept and describes it in basic terms.

An acceptable use policy **MUST BE** read and signed by everyone that uses the school systems. All signed acceptance policies are filed by the school. It is about accountability, responsibility, and respect.

The acceptable use policy is a guide for users to understand what is expected of them while using the school systems.

User Responsibilities

Please note the following

- ✓ You will not be provided with a school account to access resources until the Acceptable Use Policy is read and accepted by the user, parent/guardian.
- ✓ Your device, user account activity will be audited at regular intervals.
- ✓ All digital information stored on the school network and its IT infrastructure will be considered the property of St Joseph's RC High School
- ✓ Login activity and use of St Joseph's RC High School network are continually monitored and audited by IT Services.
- ✓ All E-mail activity is monitored and logged.
- ✓ All incoming and outgoing E-mails are scanned for harmful content.
- ✓ All Internet activity is monitored and logged.
- ✓ All data stored on the school infrastructure system is securely backed up.
- ✓ All material viewed is scanned for viruses and malware.
- ✓ All Internet content accessed is scanned to allow safe material.
- ✓ All removable media (USB memory Sticks, Thumb Drives, Flash Drives, external drives) access is restricted by the school.
- ✓ Vital IT training set by the school must be completed for the safety of the school infrastructure.
- ✓ All devices are regularly checked for damage and vandalism.

Failure to comply with the school's policies may lead to

- ✓ Account suspension
- ✓ Checking of network activity
- ✓ Checking of stored materials
- ✓ Examination of historical network activity
- ✓ Internal disciplinary action
- ✓ Possible criminal investigation

St Joseph's RC High School may add, delete, or modify this AUP at any time without notice. You are expected to check the AUP from time to time and take note of any changes that the school makes.

Overview

The Acceptable Use Policy (AUP) is composed to maintain the confidentiality, availability, and integrity of the IT infrastructure at St Joseph's RC High School in terms of maintaining an ethos of honesty, trust, and collaboration. St Joseph's RC High School is committed to protecting all stakeholders from illegal or inappropriate activities that may be executed by individuals with or without their knowledge.

IT infrastructure, including but not limited to computer equipment, software, operating systems, storage media, network accounts including E-mail and Internet browsing and data are the property of St Joseph's RC High School. These systems are to be used for the purpose of education in terms of the primary activity of the school.

Stakeholders of the system in this instance includes Students and authorised student visitors. Effective security is teamwork involving all stakeholders who access the school's information systems and associated infrastructure. It is deemed the responsibility of all system users to complete designated training, read and follow the guidelines of the AUP and to carry out their activities accordingly.

Purpose

The purpose of this policy is to outline acceptable use of the IT infrastructure at St Joseph's RC High School. These procedures are in place to protect students and all stakeholders from inappropriate activities that might compromise the IT infrastructure and the school's reputation.

All stakeholders are required to accept procedures and practices that safeguard the security, integrity and safety of information created and held by the school through the adherence of the Acceptable use policy.

Scope

This Policy applies to all stakeholders authorised to have access to the School's IT infrastructure and facilities.

This Policy applies to all St Joseph's RC High School IT services and property, whether they are located on or off site.

This Policy covers at St Joseph's RC High School IT Services infrastructure contain all:

- ✓ Physical or virtual computers to include Servers, desktops, terminals, or mobile devices.
- ✓ Peripherals such as: Monitors, keyboards, and printers.
- ✓ Computer networks, including wireless and telecommunications networks.
- ✓ Software and data held within the IT infrastructure.
- ✓ Computer-based information systems provided for education and administration.
- ✓ Devices not owned by the school which are connected to the school network and its services.

Policy

Password Creation and Use

If you are unable to access your account or for any reason, are unable to access services related to password protected systems, please contact IT SERVICES.

Location: Second Floor Next to S1

DO

- ✓ Change the default password given to you when you connect for the first time.
- ✓ Have a password with at least eight characters long and include lowercase letters, uppercase letters, numbers, and symbols.
- ✓ Consider using a passphrase instead of a password.
- ✓ Choose a password that would be hard to guess.
- ✓ Log off from your computer at the end of every session.
- ✓ Regularly change your password.
- ✓ Report phishing emails activities that ask you to reveal your password.
- ✓ Report any suspected password compromise instantly to IT Services, password should be changed quickly, and multi-factor authentication will be enabled on your account.
- ✓ Follow good security practices when choosing, using, and protecting your passwords. IT Services can reset your password if required. We will never ask you to reveal your password.
- ✓ Use authorised approved password manager to securely store and manage all related school passwords i.e. (Microsoft or Google Authenticator).

DO NOT

- Write your password down or store it in an insecure manner.
- Use another person's username and password.
- Permit or allow another person to use your username or password.
- Allow your password to become known by other users.
- Disclose your account password to others or permit use of your account by others.
- Reveal your password to someone unauthorized to gain access to our computer system.
- Have passwords that contain the username or parts of the user's full name, such as a first name.
- Use the **remember password feature** of applications (for example, web browsers)
- Insert your password into email messages without encryption or other forms of electronic communication, nor revealed over the phone to anyone.

Your username and password are the key device for access to the school's computer system, services, and network. All access and activity that is logged can be tracked back to your username.

Use of School Devices

All devices containing stored data owned by the school use an approved method of encryption to protect stored data. School devices are defined to include laptops, phones, desktop computers, mobile devices, printers, and projectors.

When using the school's computer systems, you should comply with the following guidelines. These guidelines are intended to help you make the best use of the computer resources at your disposal.

DO

- ✓ Agree to the terms and conditions of all license agreements relating to installed software or software accessed through the school network including all restrictions related to commercial use.
- ✓ Seek authorization to access, change, save or copy records or files.
- ✓ Conform to the AUP while using the school internet.
- ✓ Ensure that you log out of School systems at the end of each session.
- ✓ Protect equipment from theft.
- ✓ Refrain from eating and drinking in computer rooms and while accessing school equipment.
- ✓ Respect all elements of the IT environment and its infrastructure.
- ✓ Report all incidences of malicious damage to the classroom teacher or IT services via the IT helpdesk.
- ✓ Report all incidence of hardware or software failure to the classroom teacher or IT services via the IT Helpdesk.
- ✓ Report immediately any loss or theft of any device containing data to IT Services, room located next to S1.
- ✓ Lock the computer room when not in use.
- ✓ Inform classroom teacher or IT Services located next to S1, if the computer room codes have been compromised.

DO NOT

- Move computer equipment from room to room without approval from IT Services.
- Move any computer trolleys from room to room without approval from IT Services.
- Install unlicensed software or applications on school computers, server's laptops, or mobile devices.
- Connect devices to school systems without the consent of the IT Services.
- Install or use any personal device or software on the school computer system that bypasses security controls including monitoring and filtering.
- Bypass any security measures used to safeguard the safe processing of information on any school computing equipment, information systems or communication equipment.
- Remove or disable anti-virus software and password protection.
- Produce, access, transfer or download inappropriate or extremist materials, using the School's IT systems or network.
- Participate in harassing, slandering or other anti-social behaviors online.
- Create or spread any offensive, obscene, or rude images, data, or other material in any form.
- Use the computer system to attack or gain access to other networks, computer systems or data.
- Invade the copyright of another person or organisation.
- Leave computers screens locked for more than 30 minutes, thus stopping others from using the shared resource.
- Use, duplicate or copy software downloaded from the Internet.
- Install any software or alter its configuration, this activity may only be undertaken by the IT Services.
- Vandalize or destroy data of a different user, the operation of the network, Internet, or other network that are connected to the Internet.
- Deliberately damage computer hardware such as monitors, projectors, remotes, base units, printers, keyboards, mice, mobile devices, cables, or other hardware.
- Attempt to bypass any of the school's security and filtering systems or download any unauthorized software or applications.
- Interfere with peripheral computer systems or devices (e.g., printers and projectors) and their cabling, internal parts, or casings.
- Misuse the network in such a way to deny the services to all the rest of the users.
- Waste staff time, effort, or computer resources by storing personal photos, downloading music or films, personal online shopping, accessing social networking sites such as Facebook, legal media sharing sites.
- Stay in a computer room without the permission of teachers or IT Services.
- Eat, drink, or leave litter in any computer room, always use the bins.
- Share passwords or use memory sticks.

Malicious Code

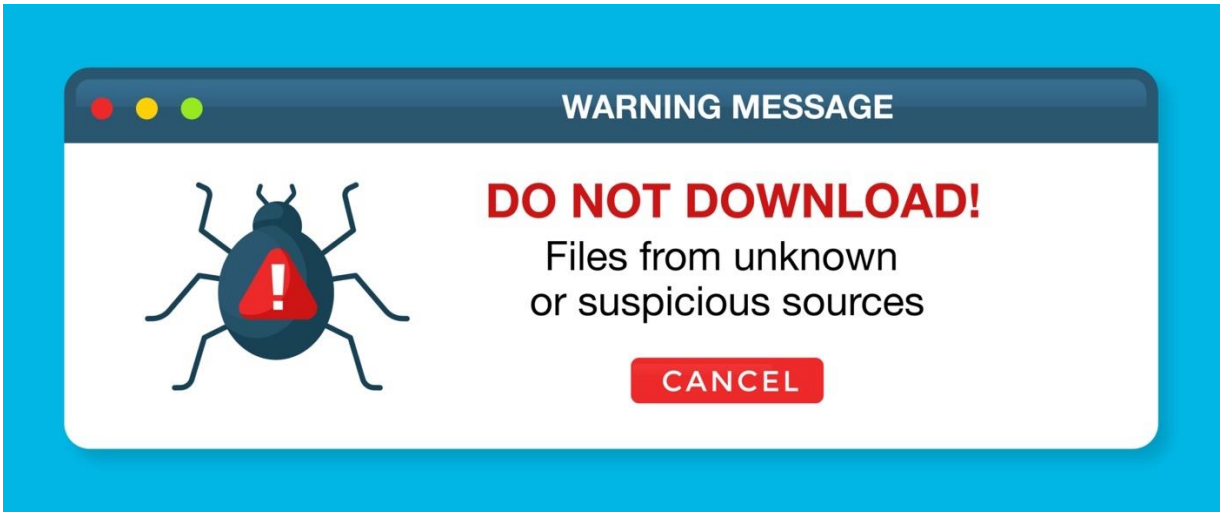
Viruses, trojans, ransomware, spyware, adware, hacking tools are categorized as malicious code and are a risk to the School Systems. Web sites that identify causes of computer viruses and malware are blocked. Users should use suitable caution when accessing Websites.

DO

- ✓ Take all necessary precautions when downloading files from the internet or attached to emails.
- ✓ Take steps to secure your computer when leaving it for a few minutes to avoid the risk of interfering or misuse e.g., by locking the screen (Windows Key + L).
- ✓ Delete, report spam, chain, and other junk email without forwarding.
- ✓ Inform IT Services immediately if you think that your computer may have a virus.
- ✓ Ensure that any equipment, not belonging to the school, used to access School systems are free from malicious code e.g., check with an up-to-date anti-virus software, the device will not be allowed on the network if no virus protection is current.

DO NOT

- × Open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- × Download files from unknown or suspicious sources.
- × Direct disk share with read/write access unless there is absolutely requirement to do so.
- × Deliberately, or carelessly allow malicious code or any other unwanted program or file onto any School systems.
- × Port or security scan the network.
- × Bypass user authentication or security of any system, network, or account.
- × Use any program, script, command, or send messages of any kind with the intent to interfere with, or disable via any means, locally or via the Internet.
- × Introduce malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- × Deliberately circumvent any precautions taken to prevent malicious code accessing School systems e.g., by disabling antivirus software.



Use of School Email System

School staff will communicate with you via email using sjhs.newport.sch.uk email address, regarding your study. The school provides E-mail accounts to students to enable them to communicate effectively and efficiently with other members of staff and students.

The school uses Office 365 for email resources. Once your account is created for office 365, you agree not to use the account to send spam, distribute viruses, or otherwise abuse the service.

DO

- ✓ Check your E-mail frequently to see if you have any messages.
- ✓ Include a meaningful subject line in your message.
- ✓ Check the address line before sending a message and check you are sending it to the right person.
- ✓ Delete E-mail messages when they are no longer required.
- ✓ Take care not to express views, which could be regarded as offensive or defamatory.
- ✓ Report Junk and Phishing emails when received.

DO NOT

- × Expect an immediate reply, the recipient might not be at their computer or could be too busy to reply straight away.
- × Forward E-mail messages sent to you personally to others, particularly newsgroups or mailing lists, without the permission of the organizers.
- × Use E-mail for personal reasons.
- × Send excessively large E-mail messages or attachments.
- × Send unnecessary messages such as celebratory greetings or other non-work items by E-mail, particularly to several people.
- × Participate in chain or pyramid messages or similar schemes.
- × Represent yourself as another person.
- × Use email for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Users who receive any emails with this content from any other users should report the matter to their teachers immediately.
- × Share passwords.

Use of School Internet

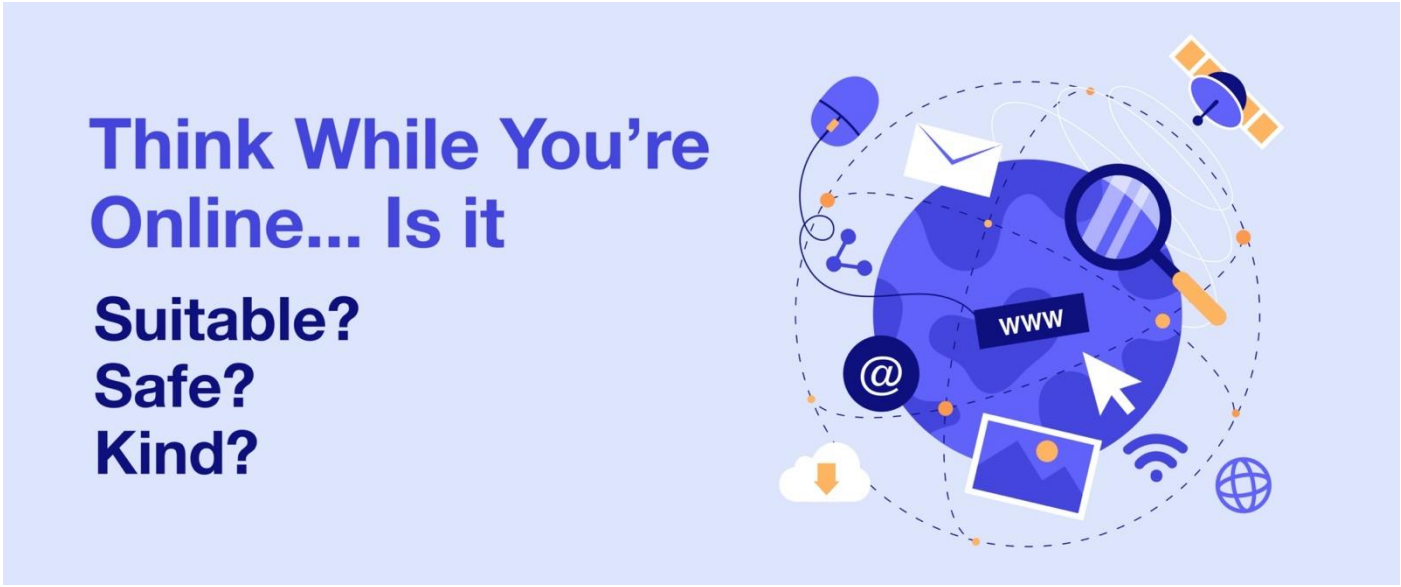
The school provides Internet access to students to assist them in their education. It is expected that it will be used to research information concerning their courses and coursework material. It should not be used for personal reasons. You may only access the Internet by using the school Web content scanning software, firewall and router.

Our systems monitor web use from any host within the network. These standards are designed to ensure users use the Internet in a safe and responsible manner and ensure that web use can be monitored or investigated during an incident. IT Services shall block access to Internet websites and protocols that are deemed inappropriate for the school.

IT Services will verify compliance to this policy through various methods, including but not limited to, periodic checks, reporting tools, internal and external audits. Internet bandwidth both within the school and in connecting to the Internet is a shared, limited resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other system users.

DO

- ✓ Keep your use of the Internet to a minimum.
- ✓ Check that any information you access on the Internet is accurate, complete, and current.
- ✓ Check for validity of information.
- ✓ Respect the legal protections to data and software provided by copyright and licenses.
- ✓ Inform IT Services immediately of any unusual incidence.
- ✓ Inform IT Services Immediately if you mistakenly access material that is profane or obscene.
- ✓ Submit a blocked site to IT Services if you require access to the site for educational purpose.



DO NOT

- Download content from Internet sites except if it is lesson/course work related.
- Download text or images which contain material of a pornographic, racist, or extreme political nature, or which incites violence, hatred, or any illegal activity.
- Download software from the Internet and install it on the school's computer system.
- Use the school's computers to make unauthorised entry into any other computer or network.
- Disrupt or interfere with other computers or network users, services, or equipment.
- Intentional disruption of the operation of computer systems and networks.
- Represent yourself as another person.
- Use Internet access to transmit confidential, political, obscene, threatening, or harassing materials.
- Arrange, over the internet, to meet strangers, or give out any of your personal information.
- Play any games or use bypass websites, order any items or services, if you are aware of any users doing this, please report it to IT Services.
- Use any proxy avoidance tools or site to bypass the school web filter
- Store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" or do so at your own risk.
- Reproduce materials available over the internet. It must be done only with permission of the author or owner of the document, unless permission from the copyright owners is first obtained, making copies of the material from magazines, journals, newsletters, other publications, and online documents is forbidden. This notion of "fair use" is in keeping with international copyright laws.

Use of Mobile Device/Trolley

Mobile devices and trolleys, such as smartphones and tablet computers, are important tools for the school and their use is supported to achieve your studies to research or check information. Each department will have a trolley stored in their preferred classroom for users to access.

DO

- ✓ Agree to the terms and conditions of all license agreements relating to installed software or software accessed through the school network including all restrictions related to commercial use.
- ✓ Return the laptop at the end of the lesson to the trolley.
- ✓ Report any damage to a device before it is returned to the trolley.
- ✓ Plug in the laptop to charge at the end of your lesson.
- ✓ Report all lost or stolen devices to IT Services immediately.
- ✓ At all times set your device to silent as not to disrupt lessons with ringtones, music, or message notifications.
- ✓ Take additional care when using mobile technology to hold school data including emails.

DO NOT

- × Move computer equipment from room to room without approval from IT Services.
- × Move any computer trolleys from room to room without approval from IT Services.
- × Load pirated software or illegal content onto mobile devices.
- × Merge personal and school email accounts on your device.
- × Use school device to backup or synchronize devise content such as media files unless such content is required for legitimate purposes.
- × Use Mobile Devices to make or receive calls, send, or receive emails / text messages, surf the internet, take images, or video or use any application during lessons, assemblies, corridors or other activities.
- × Have illegal, violent, degrading, or offensive images. The transmission of such images/information may be a criminal offense.
- × Do not charge mobile devices on school hardware or electrical systems. Ensure that mobile devices are fully charged and fit for purpose before use.

Students will be held accountable for any loss or damage to hardware devices. Students/parents could be asked to pay for the cost of repair or replacement if deemed necessary by the school.

Use of Wireless Communication

The school runs Wi-Fi and allows access for education, research, and revision. Access to the WI-FI network is available throughout the school and is accessed on the school owned mobile devices.

Currently this is restricted to School Mobile devices only.

When using Wi-Fi, you are subject to and expected to comply with the AUP.

The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

The use of the school Wi-Fi will be safe and responsible and will always be in accordance with the School AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

DO

- ✓ Access for school-related activities only.
- ✓ Have up-to-date Anti-Virus software & definitions installed.
- ✓ Use your own network logon credentials – All Wi-Fi use will be the responsibility of the authenticated user.

DO NOT

- × Access Wi-Fi if you are not using school devices.
- × Attempt to bypass the school systems is strictly forbidden and will be treated as an attempt to hack the network.
- × Permit to act as a Hotspot or a Repeater/Relay.

Use of social media

Facebook, Twitter, Instagram, TikTok, email and other online social networks play a key part in the lives of students. Given the rapid increase of social media, it is impossible to list all possible types of media as they are constantly increasing. School students are not permitted to access social media websites from the school's computers or other school devices at any time, except authorised by The Head Teacher.

The school appreciates that students may use social media in a personal capacity. However, students must be aware that if they are known from their user profile as being related with the school, views they express could be considered to reflect the school's opinions and so can damage the name of the school.

For this reason, they should avoid mentioning the school by name, or any member of staff by name or position or any details relating to the school. Opinions offered should not bring the school into disrepute, breach confidentiality or copyright, or bully, harass, or discriminate in any way.

Communicates to all students and to all online communications which directly or indirectly, represent the school, and to such online communications posted at any time and from anywhere. If a school user carelessly takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

DO

- ✓ Consider the copyright of the content you are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- ✓ Ensure that use of social media does not infringe upon relevant data protection laws, or breach confidentiality.
- ✓ Report to IT Services if inappropriate content is accessed online on school premises.
- ✓ Verify links, attachments, downloads, emails, or any other received items.

DO NOT

- Access social media in school.
- Create or transmit material that might be defamatory or incur liability for the school.
- Post messages, status updates or links to material or contact that is inappropriate.
- Upload pictures online other than via school owned social media accounts.
- Disclose any confidential information to third parties.
- Link to your own blog or other personal web pages to the school website
- Make comments, post content or link to materials that will bring the school into disrepute.
- Give away your password or use the same password for any other services.
- Post content that could easily be viewed as obscene, threatening or intimidating or even might constitute harassment or bullying.
- Publish confidential or commercially sensitive material.
- Breach copyright, data protection or other relevant legislation.
- Attempt to bypass the network's firewalls to access social media.
- Give out personal information, or post personal images to people you talk to online.
- Arrange to meet somebody you have only met online.
- Believe everything you read, verify sources and content of information.
- Create social media accounts with school logo.

Use of Microsoft Office 365/Google Workspace

Microsoft Teams/Google Workspace are applications that allows you to create, share and collaborate online. They are the official communication and collaboration tools at St Joseph's RC High School. It is used for remote teaching and is supported by the school AUP. This application can help you attend your classes online, submit homework/coursework, participate in discussion, chatting, and viewing your teachers screen in real time.

School MS Teams/Google Workspace are provided for use in relation to school activity e.g., to support discussions, collaboration and communication relating to study; engagement, events, and activities; and internal staff peer networks.

MS Teams sites/Google Workspace are provided to include members selected from across our student and staff community. Guest access can be arranged for third parties working outside of the school. For further guidance please contact IT Services.

MS Teams/Google Workspace are Cloud Services and therefore information contained within our school Domain sites is stored in Data Centres. This meets UK and EU data protection and security standards.

Interaction is encouraged. Chat-based collaboration is a useful tool when there is regular interaction and works best when there are multiple voices represented within the dialogue. It is important that users recognise that this is a school provisioned service and therefore users must adhere to the guidance below or risk disciplinary action. Usage may therefore differ to the way you engage within external collaborative or social media sites designed for personal use.

DO

- ✓ Use your own name and photograph within your office 365 profile/Google Workspace. It is important that members are clear about who they are interacting with.
- ✓ Post to appropriate users
- ✓ Stay on topic and avoid sharing irrelevant content, No spam.
- ✓ Remember that all chat content, whether direct or within channels is searchable.
- ✓ Remote learning will only take place using Microsoft TEAMS for Education
- ✓ Think carefully about what acceptable language with regards is to what you type and post.
- ✓ Hang up at the end of the lesson once instructed to do so. The teacher is responsible for ensuring the meeting is closed.

DO NOT

- × Disclose personal information and protect yourself against identity theft.
- × Create separate channels for private one-to-one chats or group chats.
- × Do not share sensitive information through the chat.
- × Share images and videos that breach image rights and copyrights. Seek permission from your teacher prior to sharing them.
- × Use a personal account to communicate with teachers
- × Attempt to call, chat or setup private groups
- × Attempt to start or record a meeting/lesson (this feature has been disabled)
- × Share recorded videos or lessons made by teachers within or outside of your team's account

Monitoring

The school maintains the right to examine any systems and inspect any data recorded in those systems. To ensure compliance with this policy, the school will use monitoring software to check upon the use and content of emails periodically. Such monitoring is for legitimate purposes only.

If the School suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school will terminate or restrict usage. If the School suspects that the system is be being used for criminal purposes, then the matter may be brought to the attention of the relevant law enforcement organisation.

Leaving School

Student school profiles will be suspended and subsequently deleted when students either move to another educational establishment or terminate their studies at the school.

You must make all efforts to transfer important files from your school file space before you terminate your studies at the school. No responsibility will be taken by the school for the loss of data deleted in respect to the termination of study and deletion of student accounts.

If you discover a security problem, for example being able to access other user's data, you must inform IT Services immediately and not show it to other users. Students known as a security risk will be denied access to the network.

Penalties

Non-Compliance

Failure to comply with these rules will result in one or more of the following: -

- A ban, temporary or permanent on the use of the Internet services at the school
- A letter notifying your parents of the nature and violation of the policy
- Appropriate actions and restrictions placed on access to the school resources to be decided by the Head of Year/ Head of Department
- Any other action decided by the Headteacher and Governors.

Use and Access to school resources and information is conditional upon adherence to the Acceptable Use Policy. Where there is found to have been a deliberate attempt at unauthorised access or mindful carelessness to protect the school information systems and data, the school will initiate the appropriate disciplinary processes.

It is your responsibility to report suspected breaches of security policy without delay to IT Services. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with St Joseph's RC High School disciplinary procedures.

Disciplinary role can vary depending upon the severity of the offence, from a recorded verbal warning, written warning, temporary withdrawal of internet use, suspension of all account activity to school exclusion. Any breach of any law may lead to criminal proceeding.

Exceptions

Any exception to the policy must be approved by the Business Manager, IT Manager and Head teacher in advance.

External documents

https://www.legislation.gov.uk/

All users must conform to all applicable regulation and legal precedent, including the requirements of the following specifically related Acts of Parliament, or any reform thereof:

requirements of the following specifically related Acts of Parliament, or any reform thereof:

- Malicious Communications Act 1988
- Computer Misuse Act 1990
- General Data Protection Regulations
- The copyright, designs and patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Communications Act 2003
- Counterterrorism and Security Act (2015)
- Google Cloud APPS AUP

- SANS
- FOI Digital Safety Policy
- UK General Data Protection Regulation (UK GDPR)
- Privacy Notice
- Information Commissioner's Office (ICO)

Revision History

This policy is reviewed regularly and may be subject to change.

Date of Change	Responsible	Summary change
May 2023	IT Services	Updated and converted to new format