User Responsibilities

Please note the following

- **Your computer and account activity will be audited periodically.**
- **All data and material stored on the school network and its servers will be considered the property of St Julian's school.**
- **Logins activity and use of St Julian's School network are monitored and audited regularly by IT services.**
- **All E-mail activity is monitored and logged.**
- **All incoming and outgoing E-mails are scanned for viruses.**
- **All Internet activity is monitored and logged.**
- **All material viewed is scanned for viruses and malware.**
- **All Internet content viewed is scanned for offensive material.**

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 Julian's 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 St Julian's School makes

1. Overview

The Acceptable Use Policy (AUP) is set in place to uphold the integrity of IT systems in St Julian's School in terms of maintaining an ethos of honesty, trust and collaboration. St Julian's School is committed to protecting all stakeholders from illegal or inappropriate activities that may be perpetrated by individuals with or without their knowledge.

IT systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing E-mail and Internet browsing are the property of St Julian's School. These systems are to be used for purpose of education in terms of the primary business activity of the organisation. Stakeholders of the system in this instance include: Students and authorised student visitors.

Effective security is team work involving all stakeholders who access the schools information systems and associated infrastructure. It is deemed the responsibility of all system users to read and follow the guidelines of the AUP and to conduct their activities accordingly.

2. Purpose

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

All stakeholders are required to accept procedures and practices that safeguard the security, integrity and safety of information created and held by St Julian's school through the adherence of the AUP.

3. Scope

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

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

For the purpose of this Policy, St Julian's School IT Services facilities 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 St Julian's School which are connected to the School network and its services.

4. Policy

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

✓ **Use of School Computer Equipment**

☑ **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 authorisation to access, change, save or copy records/files and computer records.
- Conform to the AUP while using a 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 suites and while accessing school equipment.
- Respect all elements of the IT environment and its infrastructure.
- Report all incidences of malicious damage to appropriate teaching staff or IT services.
- Report all incidence of hardware/software failure to appropriate teaching staff or IT services.

☒ **DO NOT**

- Move computer equipment from room to room without approval from IT Services
- Install unlicensed software or applications on school computers, server's laptops or mobile devices.
- Connect phones to a school device without the consent of the IT Services
- Install or use any 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/disable of anti-virus software and password protection is prohibited.
- 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 behaviours 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 unauthorised access to other networks, computer systems or data.
- Invade the copyright of another person or organisation
- Leave computers screens locked for more than 20 minutes, thus stopping others from using the shared resource.
- Use shareware or similar software downloaded from the Internet.
- Duplicate or copy software.
- Install any software on your machine or alter its configuration, this activity may only be undertaken by the IT Services.

- Vandalise 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, base units, printers, keyboards, mice, mobile devices or other hardware
- Attempt to bypass any of the School's security and filtering systems or download any unauthorised software or applications.
- Interfere with peripheral computer systems or devices (e.g. printers and projectors) and their cabling, internal parts or casings.

The School has a legal obligation to take steps to prevent individuals being drawn into extremism and terrorism, and a duty to alert and report any attempted access to, or distribution of, such unsuitable material.

✓ **Use of Passwords and Access**

If you are unable to access your account or for any reason are unable to access services related to password protected systems contact IT SERVICES
Location: Jubilee Block by J29

☑ **DO**

- Change the default password given to you when you connect to the network, application or system for the first time.
- Have a password with at least eight characters long.
- Have a Passwords with at least three of the four available character types: 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.
- Check emails for phishing activities that ask you to reveal your password.
- Report any suspected password compromise instantly to IT Services, and password should be changed quickly.
- 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

☒ **DO NOT**

- Write your password down or store it in an insecure manner.
- Use another person's username.
- Permit or allow another person to use your username/password.
- Allow your password to become known by another users
- Disclose your account password to others or permit use of your account by others.
- Reveal your password to someone unauthorised in order to gain access to our computer system
- Have a Passwords that contain the user name or parts of the user's full name, such as a first name

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

✓ Viruses and Malicious Code

Viruses, spyware, hacking tools are categorised as malicious code and are a risk to St Julian's School Network System. Web sites that are identified causes of computer viruses and malware are blocked. Users should use suitable caution when accessing Web sites.

☑ 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.
- Make sure that every CD, DVD and USB stick to be used on the school system are virus checked before use.
- Delete 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 you use to access School systems are free from malicious code e.g. check with an up to date anti-virus software

☒ DO NOT

- Deliberately, or carelessly allow malicious code or any other unwanted program or file onto any School systems.
- Port, 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
- Open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then empty your deleted items

✓ Use of School E-Mail

St Julian's School staff will correspond with by email using **Stjuliansschool.co.uk** email address, regarding your study. The School provides E-mail to students to enable them to communicate effectively and efficiently with other members of staff and students.

St Julian's School uses Google Apps for Education. Once you sign up for a G Suite account, you agree not to use the account to send spam, distribute viruses, or otherwise abuse the service. All users on St Julian's School are subject to these agreements, which are part of the G Suite **Acceptable Use Policy**.

When using St Julian's School Google E-mail facilities you should comply with the following:

☑ DO

- Check your E-mail regularly 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.
- Respect the legal protections to data and software provided by Google Cloud copyright and licenses.
- Take care not to express views, which could be regarded as offensive or defamatory.

☒ 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 originator.
- 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 electronic mail to send or forward material that could be construed as confidential, political, obscene, threatening, offensive or defamatory.

✓ Use of School Internet

St Julian's 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 St Julian's Web content scanning software, firewall and router.

☑ 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.

☒ DO NOT

- Download content from Internet sites except if it is 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.
- Access unauthorised chat rooms.

✓ Use of Social Media

Facebook, Twitter, 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.

St Julian's 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 student's may use social media in a personal capacity. However, student 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 users 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 message, 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, very sources and content of information.

✓ Use of Mobile devices

Mobile devices, such as smartphones and tablet computers, are important tools for the School and their use is supported to achieve your studies.

It is the responsibility of each student who chooses to bring a mobile device into school to abide by the rules laid out in this policy and in accordance with the AUP.

However mobile devices also represent a major risk to information security and data security as, if the appropriate security applications and procedures are not applied, they can be a channel for unauthorised access to the School data and IT infrastructure.

Wi-Fi Internet Access configuration. This service is limited to **Post 16 Students Only**

☑ DO

- Report all lost or stolen devices to IT Services immediately.
- Ensure the adequate physical security of the device.
- 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 technologies to hold School data (including email) or access systems.
- Obey to the additional controls and requirements set out for Mobile Devices.

☒ DO NOT

- Connect your device directly to the internal corporate network.
- Jailbroke or have any software or firmware installed which is designed to gain access to or is entered to be exposed to the user.
- Load pirated software or illegal content onto Mobile devices.
- Merge personal and school email accounts on devices.
- 'Jailbreak' a school iPad.
- Use School computers to backup or synchronise device 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 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 and the students/parents could be asked to pay a charge if deemed necessary by the school

✓ Use of Wi-Fi

St Julian's School provides Wi-Fi and allows access for education, research and revision. Access to the WI-FI network is available throughout the School and is accessed using the "St Julian's Post 16" SSID where users will need to logon using their School username and password. Currently this is restricted to **Post 16 students only**. The school accepts no responsibility for any Hardware or Software loss or damage, occurring within the school and through use of the School's Wi-Fi network.

☑ DO

- Access for school related activities.
- 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 a Post 16 student.
- 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.

When using the Wi-Fi, even if it is with your own device, 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.

✓ Use of Remote Access

All remote access will be managed by St Julian's School IT Services and will utilize encryption and strong authentication measures.

It is the responsibility of any Student of St Julian's School with remote access privileges to ensure that their remote access connection remains safe. It is vital that any remote access connection used to conduct St Julian's school work be utilized appropriately, responsibly, and properly.

All students of the St Julian's school shall only connect to or have access to machines and resources that they have permission and rights to use.

Students also agrees to and accepts that access or connection to St Julian's School networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity order to identify accounts/computers that may have been compromised by external parties

☑ DO

- Ensure that your device is updated with the most recent security patches for their Operating System when accessing remote
- Immediately report to IT Services any incident or suspected incidents of unauthorized access and/or disclosure of School resources, networks, etc.
- Accept that connection to St Julian's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.
- Take reasonable steps to ensure that any Remote Access to the LAN is treated with the same security approach as a connection made within the School.
- Report immediately, to IT Services any incident or suspected incidents of unauthorized access and/or disclosure of School resources, databases, networks, etc.
- Ensure that your remote access connection is given the same consideration as the Students' on-site connection to St Julian's School.

☒ DO NOT

- Use Internet access through School networks via remote connection for the purpose of illegal transactions, harassment, competitor interests, or obscene behaviour, in accordance with other existing policies.
- Make modifications of any kind to the remote access connection without the direct approval of IT Services.
- Use Internet access through School networks via Remote access connection for the purpose of illegal transactions, harassment, interests, or obscene behaviour.
- Give access to household members through the St Julian's School Remote access.

✓ **Leaving School**

Student school profiles will be suspended and subsequently deleted when students either move to another educational establishments or terminate their studies at St Julian's school.

You must make all efforts to transfer important files from your School file space before you terminate you studies at St Julian's 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

✓ **Monitoring**

The school maintains the right to examine any systems and inspect any data recorded in those systems. In order to ensure compliance with this policy, the school will use monitoring software in order 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 may be being used for criminal purposes then the matter may be brought to the attention of the relevant law enforcement organisation.

✓ **Disciplinary Process**

Non-Compliance

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 wilful 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 Julian's school disciplinary procedures.

Disciplinary 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 Network Manager and Head teacher in advance.

5.0 External documents

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:

- Malicious Communications Act 1988
- Computer Misuse Act 1990
- Data Protection Act 1998
- 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
- Counter-Terrorism and Security Act (2015)
- Google Cloud APPS AUP - https://cloud.google.com/terms/aup
- SANS- https://uk.sans.org/

Revision History

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

Date of change	Responsible	Summary of Change
March 2017	IT Services	Research, Updated and converted to new format
April 2017	HOD ICT	Review