Please note the following

- **Your computer and account activity will be audited periodically.**
- **All data and material stored on the school network and its systems 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: **Staff, Governors and 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 staff 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 St Julian's School's computer network you should conform 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**

- Report any damaged or inoperable equipment via the IT Helpdesk immediately
- Use the IT Helpdesk to report IT related issues as a first point of contact.
- Inform IT Services Immediately in the event of loss or misplaced equipment.
- Conform to the terms and conditions of all license agreements relating to any software installed on, or accessed by, St Julian's School Network including restrictions placed for commercial use.
- Only access, change, save or copy records or files where you have been given authorisation.
- Ensure that you log out of St Julian's School systems at the end of each session and check that the log out procedure has been completed successfully.
- Protect equipment from theft lock doors and ensure that no easy access to equipment is made available.
- Do not leave computer equipment unattended and accessible to the wider community.
- Avoid the consumption of food and drink at computer work stations.
- Look after all computer equipment/systems and ensure equipment is used correctly and appropriately.
- Understand that your username and password offers you access to systems and information that other staff are restricted from accessing.
- Under no circumstances allow access to a computer logged in with your credentials.
- Report to IT Services if you suspect a computer or a removable storage device contains a virus, spyware or other malware.
- Print only work that you need, where possible use email, shared folders and encrypted media to share information.
- Save work frequently using sensible file names.
- Manage and organise folders and files effectively in home directories and shared drives on a routine basis.
- Make regular backups of work in home directories, shared directories and for personal safety.
- Follow common sense health and safety guidelines where possible when using IT equipment.
- Seek guidance from Network Manager before ordering any IT equipment for your department
- Ensure the privacy of data, do not project sensitive information through other forms media such as projectors and smart screens in inappropriate environments such as live classrooms.

☒ DO NOT

- Attempt to connect to another user's laptop or device.
- Share personal details with any student at any time.
- Move computer equipment without approval from IT Services.
- Install unlicensed software or applications on school computers, servers' laptops or mobile devices.
- Install or use any device or software on school computer systems that bypasses security controls including monitoring and filtering
- Bypass any security measures used to safeguard the safe process of computing equipment, information systems or communications equipment **e.g**. disabling anti-virus software or removing password protections.
- Produce, access, transfer or download inappropriate or extremist materials.
- Participate in harassing, slandering or other anti-social behaviours online.
- Create or spread any offensive, obscene or rude images, data or other material.
- Use the computer system to attack or gain unauthorised access to other network, computer systems or data.
- Invade the copyright of another person or organisation.
- Leave computers screen unlocked when leaving the device unattended.
- Use shareware downloaded from the Internet.
- Install any software on your machine or alter its configuration, this activity may only be undertaken by the IT Services.
- Vandalise or destroy data that is not your property.
- Vandalise the network operation, Internet or other network services linked to the IT infrastructure.
- Deliberately damage computer hardware such as monitors, base units, printers, keyboards, mice, Mobile devices or other hardware.
- Attempt to bypass any security and filtering systems or download any unauthorised software or application.
- Interfere with computer systems or devices and their cabling, internal parts or casings.
- Store, download or distribute music, video or image files on Home directories or shared areas unless they are copyright free media files.
- Send or post defamatory or malicious information about St Julian's school.
- Send or post defamatory or malicious information about Individuals.

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.
Any damages to equipment will be charged to the relevant department, unless it is a proven fault with the devices.

✓ 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 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 all Staff 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 is used to conduct St Julian's business in an appropriate manner.

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

Staff 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.
- 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 system
- Report immediately, to IT Services any incident or suspected incidents of unauthorized access and/or disclosure of School resources, databases, networks and software.
- Ensure that your remote access connection is given the same consideration as the Staff on-site connection to St Julian's School network.

☒ DO NOT

- Use the Internet access via a remote access connection for the purpose of illegal transactions, harassment 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.
- Give access to household members through the St Julian's School Remote access

✓ Data Protection

☑ DO

- Support and promote e-Safety and Data Security policies and help Students to be safe and responsible in their use of IT and of related technologies.
- Use an encrypted storage device such as a USB drive encrypted using BitLocker to transfer data protected files between home and school.
- Remote access when possible rather than moving files physically from site to site using removable storage.
- Ensure that you are aware of data protection issues and understand what is considered to be classed as personal data.
- Ensure the accuracy and validity of information and data recorded in the schools MIS and administration systems.
- Ensure integrity and security of information by abiding to the AUP policies on password usage and password protection.
- Ensure the safety of sensitive information stored on mobile devices while in transit

☒ DO NOT

- Share data protected information with third party organisations without seeking advice/permission.
- Display sensitive information or personal data on a public display or projected image e.g. a smartboard. This includes learner data in SIMS.net
- Leave a computer logged on and unattended for even a short space of time in an insecure environment.
- Take sensitive data off site without relevant approval.

Ensure that personal data such as data held on SIMs.net is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head teacher or Network Manager. Personal or sensitive data taken off site must be encrypted.

✓ Use of School E-Mail

St Julian's School staff will correspond by email using **Stjuliansschool.co.uk** email address. 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

- Know that @stjuliansschool.co.uk E-mail is a work e-mail account, and as such will be used for professional purposes. Personal or home email systems should never be used for school business.
- Include a meaningful subject line in your message.
- Only open attachments or download files from trusted sources.
- Check your E-mail regularly to see if you have any messages.
- Not view, download or distribute material that could be considered offensive or pornographic.
- 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.
- Give out personal details, such as mobile phone number and personal E-mail address, to students.

✓ Use of School Internet

St Julian's School provides Internet access to stakeholders to assist them in their education. It is expected that it will be used to research information, teaching 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 disrupt the operation of computer systems and networks
  - Represent yourself as another person.
  - Use Internet access to transmit confidential, political, obscene, threatening, or harassing materials

✓ Use of Social Media

Facebook, Twitter, email and other online social networks play a key part in our lives. 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 Staff, Governors and Visitors are not permitted to access social media websites from St Julian's school's computers or other school devices at any time, except authorised by Network Manager, Head Teacher.

St Julian's school appreciates that Staff, Governors and Visitors may use social media in a personal capacity. However they 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 reputation 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.

☑ 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 and other material received via social media.
- Ensure that any personal social networking accounts that you have do not compromise the professional reputation of the school and are not used or accessed in School Working hours.

☒ DO NOT

- Access social media in school.
- Create or transmit material that might be defamatory or incur liability for the School.
- Use social networking sites to communicate with Students and parents or carers.
- Post message, status updates, links to material and contacts that may be deemed inappropriate.
- Upload pictures online other than via school owned social media accounts.
- Comment or post inappropriately information about the school.
- Disclose any information confidential to school 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.
- Breach copyright, data protection or other relevant legislation.
- Attempt to befriend or otherwise contact Students through social media.
- Post content online which is damaging to the school or any of its staff or students.
- Attempt to bypass the network's firewalls to access social media.

- Give out personal information, or post images of yourself to people you communicate with online.
- Believe everything you read, check the validity and verify all sources of all online information.
- Load photos or videos of staff and Students to websites or social networking sites.

- **If I have control over a school Twitter account**

- **Keep it as a protected account at all times**
- **Change the Password regularly**
- **Maintain the highest standards of professionalism**
- **Inform Network Manager straight away if you suspect or have lost the password**
- **Never use the account to send Direct Messages to anyone**

If you are aware of misuse of Social Networking accounts or sites that are associated with a member of staff, student or the school, You will inform the Head Teacher or Network Manager immediately

✓ **Use of Laptop Devices**

St Julian's School wishes to ensure that all Staff, Governors have access to suitable mobile computing resources in order to deliver high quality education to the students at the school. The school reserves the right to transfer the Laptop to another teacher if the teacher does not, or is unable to, for any reason, to fulfil the requirements of this Agreement.

- **DO**

  - Use the Laptop for work use only.
  - Use the laptop outside work hours.
  - Use your laptop computer home and to work from home.
  - Always have your laptop for work.
  - Return your laptop to the school at the end of each academic year, or earlier if employment is ended.
  - Approval from the school will be required if the laptop is borrowed during periods of holiday for professional purposes.
  - Take sufficient care and security safeguards when using your Laptop.
  - Report any damage or loss of the laptop to IT Services Immediately.
  - Refer any problems in using the laptop to IT Services.

☒ **DO NOT**

  - Allow students, family members or any other individual to use your laptop.
  - Leave your laptop in an unlocked room, unsecured overnight at school nor in any car while the car is unoccupied.

Departments will be held accountable for any loss or damage to any device equipment and the Department could be asked to pay a charge if deemed necessary by the school

✓ Use of Mobile devices

This applies to, but is not limited to, any device that is used for St Julian's School access. The device type are focused on Bring Your Own Device (BYOD) to work, and also impact on any mobile device provided by the School.

These devices can include:

- Smartphone (of any type)
- Mobile phones
- Any style of tablet computers
- PCs, Notebook or Laptop (or any device that has access to the School network)
- Portable media devices, chrome books

Mobile devices, such as smartphones and tablet computers and your Laptop, are important tools for the School and to teach your lessons. It is the responsibility of each member of staff, visitor, governor 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.

☑ DO

Before a device can be connected to the School network, the Staff, Governor, Visitor must obtain an approval from IT Services. We can terminate a device connection at any time for any reason.

- Report all lost or stolen devices to IT Services immediately.
- Ensure adequate physical security of the device.
- 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.
- Only install apps from trusted locations.

☒ DO NOT

- Jailbroke or have any software or firmware installed which is designed to gain access to or is entered to be exposed the school to unacceptable risk.
- Use the device to run a personal business and/or for any personal use while connected to the school network.
- Load pirated software or illegal content onto Mobile devices.
- Merge personal and school email accounts on devices.
- Use School computers to backup or synchronise device content such as media files unless such content is required for legitimate purposes.
- Have illegal, violent, degrading or offensive images. The transmission of such images/information may be a criminal offense.

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

✓ Use of Wi-Fi Network

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 Teacher" or "St Julian's Guest WiFi" SSID where Staff, Governors and visitors will need to logon using their username and password. 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. St Julian's School will monitor the network for rogue Wireless implementations and these will be disabled and disconnected immediately upon detection.

☑ DO

- Access Wi-Fi 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

- 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.
- Download, share or exchanging illegal data using St Julian's school WIFI.

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 agreement 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.

Wi-Fi permission is valid only for registered Staff, Governors. Users can connect only one device at once. The Wi-Fi access is activated automatically, as Staff, Governors registered and the login with the password. Visitors Wi-Fi will need to be requested in advance to activate the account

All relevant AUP, regulations and policies apply

✓ **Leaving School**

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

You must make all efforts to transfer important files from your School file space before you terminate your employment 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 employment and deletion of staff 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. Stakeholders 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
January 2017	IT Services	Updated and converted to new format
April 2017	HOD ICT	Review