Thornleigh
Salesian College

ICT Acceptable Use Policy

Person Responsible:	AAHT Whole School ICT
Last Reviewed:	October 2023
Adopted:	December 2022
Next Review due:	October 2025

1. Introduction

The purpose of this policy is to ensure that all users (including but not limited to Employees, Students, Visitors, Contractors) of Thornleigh Salesian College (referred to as 'the school') ICT facilities are aware of school policies relating to their use.

The school encourages the use of Information Technologies (referred to as 'ICT Facilities') for the benefit of its users. ICT Facilities are provided to support staff & students, specifically for educational, training, administrative or research purposes. This policy has been created to ensure a safe & secure IT environment for all members of the school community.

It is the responsibility of all users of school ICT facilities to be aware of and follow school ICT policies and guidelines and to seek advice in case of suspected or apparent misuse.

Users are required to agree to the methods, practices and restrictions outlined within this policy before accessing school ICT Facilities and logging in to the schools' networks and systems quantifies acceptance of this policy.

For ease of use, a simplified student agreement is supplied as an easy reference for everyday usage and disciplinary matters.

2. ICT Facilities

2.1 ICT facilities are managed by IT Support. Use of ICT facilities is at the discretion of the Senior Leadership Team (referred to as 'SLT'), and the Network Manager.

2.2 **Definitions**

2.2.1 The phrase 'ICT Facilities' as used in school policies should be interpreted broadly as including any ICT hardware (both desktop and portable), printers, telephones, or software/online services owned or operated by the school, including any allocation of storage on any local or cloud-based school systems.

2.3 **Ownership**

2.3.1 ICT facilities owned by the school and software and/or data developed or created (for whatever reason) on that equipment remains in all respect's property of the school. The Patents Act 1977 and Copyright, Design and Patents Act 1998 provide for the Intellectual Property Rights (IPR) in that work created by an employee in the course of his/her employment is vested automatically to the employer.

2.4 **End User Devices (Desktop PCs / Laptops / Mobile Devices)**

2.4.1 End User Devices are a critical asset to the school and must be managed carefully to maintain security, data integrity and efficiency.

2.4.2 IT Support has measures in place to prevent the installation of software. Users should not attempt to install non-standard software on school devices. Any software installation requests must be submitted to IT Support.

2.4.3 All users have access to appropriate areas on the school's file servers and a cloud-based system: google-drive for the secure storage of school /work related files.

2.4.4 Laptop & Mobile devices are at high risk of loss or theft and require additional security protection. All reasonable precautions must be taken to ensure that the hardware is stored securely both on and off-site.

2.4.5 To protect the integrity of the school systems and data procedures, passwords or authentication devices for gaining remote access to the school systems must not be stored with the computer. This includes the saving of passwords into remote access software.

2.4.6 Confidential data is not to be taken offsite via removable media / etc. Remote Access provides a secure Remote Desktop System that is encrypted and secure. If there is a requirement to take any confidential data offsite then please discuss with the Network Manager, to ensure the school's GDPR obligations as a Data Controller are met.

2.4.7 In event of loss or theft of a device you should report the matter promptly to the Director of School Services & the Network Manager. IT Support reserve the right to remotely locate, revoke access to and/or initiate a remote wipe of school-managed devices or accounts.

2.5 **Loan Equipment**

2.5.1 The policy regarding loan equipment is similar to that for laptops and mobile devices. Most loan equipment is highly portable and attractive to thieves. Users who borrow loan equipment must complete an Equipment Loan Form, co-signed by a member of IT Support. The User then bears responsibility for the equipment detailed therein. Loan equipment should be stored securely when not in use.

2.5.2 If loan equipment is lost or stolen the user responsible should report the matter promptly to IT Support to enable loss/theft procedures detailed in 2.4.7.

2.5.3 If loan equipment incurs damage, please inform the Network Manager – users should not attempt to fix or have the device repaired themselves. In the event of damage, repair/replacement charges may be applied at the discretion of the Senior Leadership Team.

2.6 **ICT Disposal**

2.6.1 All ICT equipment is disposed of by IT Support using a WEEE-certified disposal company. Disposal documentation is retained by IT Support. Under no circumstances may users dispose of equipment themselves.

2.7 **Software & Managed Services**

2.7.1 All software present on school Devices has been assessed and verified for use by IT Support. Users should not attempt to install non-standard software on school devices. IT Support has measures in place to prevent the installation of software on school-owned devices. If additional software is required a purchase and/or installation request must be submitted to IT Support via the Helpdesk.

2.7.2 All purchase orders for software should be submitted to IT Support prior to purchase to ensure compatibility and avoid duplication of services. The use of unverified or unauthorised software can cause unforeseen problems with school IVT facilities.

2.7.3 Mobile Apps loaded onto school owned mobile devices that are deemed 'on loan' are the responsibility of the user in terms of configuration and licensing unless otherwise agreed by IT Support. IT Support cannot guarantee support for apps purchased without prior consultation.

2.8 **Network Access & Data Storage**

2.8.1 In order to use the IVT facilities of the school a person must first be provided with their own unique User Account by IT Support. Access to IVT facilities implies and is conditional upon, acceptance of this Acceptable Use Policy. Staff and Student user accounts are automatically generated when a record is added to the school MIS System. Accounts for additional systems and external managed services are generated and managed by IT Support unless otherwise stated.

2.8.2 All individually allocated usernames and passwords are for the exclusive use of the individual to whom they are allocated. Passwords protect the school's systems from access by unauthorised people; they are for the protection of all school systems and data held within them. Users are personally responsible and accountable for all activities carried out under their user account. This applies to all school-based and externally hosted/externally managed services.

2.8.3 Passwords for personal user accounts must never be divulged to another person. If a password is forgotten or misplaced, a member of IT Support can assist in reset / recovery measures. Attempts to access, or use, any user account, which is not authorised to the user are strictly prohibited.

2.8.4 Passwords should be suitably complex so as not to be guessed easily. IT Support enforce basic password requirements on the school Network that reflect real-world practices found on most common websites and services including recommendations from the National Cyber Security Centre. The requirements for the school Network and associated services are:

1. Passwords must be at least twelve characters in length.

2. Passwords must not contain the elements of the user's real name or account username eg. Their forename or surname.

2.8.5 All staff computers have a time-out function which will lock the device when left idle for 10 minutes, however, staff should ensure that teaching PCs are locked when leaving the classroom, likewise, classrooms with computers should be locked when leaving the classroom to ensure data security.

2.8.6 Mobile and Tablet devices should have a passcode / biometric login to protect data on a device. It is also recommended that personal staff devices that are brought into school have similar protection.

2.8.7 Wi-Fi access for guests, staff and students is provided on a secure, segregated wireless network, access to which is at the discretion of Senior Leadership Team and IT Support. ICT hardware/equipment not owned by the school may not be connected directly to the internal school network without prior written request and technical approval by IT Support. All external devices must register on the guest / staff / sixthform network before use. This records users IP address; name and contact details through the Wifi registration page when accessing the network for the first time; at the same point users will need to agree to the acceptable usage policy. All users will need to reaccept the policy and give their details each quarter.

2.8.8 It is school policy to store User Data on designated file servers. These servers are regularly backed up to secure recovery locations using industry-standard backup software.

Users should store data appropriately dependent on its purpose and in accordance with relevant government legislation. User accounts are each allocated a secure 'My Documents' mapped drive along with appropriate access to secure network locations depending on their role within the school. It is each user's responsibility to store data appropriately. If you require further information regarding appropriate data storage please contact the Director of School Services or the Network Manager.

2.8.9 The School maintains a notification with the Information Commissioner's Office in compliance with the General Data Protection Regulation 2018. It is the responsibility of all school staff to ensure that personal data held and processed is within the terms of the school's data protection policy.

2.8.10 The school reserves the right to access any User Data held within ICT Facilities and/or externally hosted school systems when deemed appropriate by Senior Leadership.

2.8.11 Staff & Student Accounts are automatically disabled within 24 hours of the account holder being marked as 'Leaver' within the school MIS System. Secure User areas relating to leavers are securely retained as part of the school backup policy and in accordance with Data Protection Legislation.

2.8.12 Account access can be restored to users for limited periods when deemed appropriate by Senior Leadership / IT Support. If you require account access after officially leaving Thornleigh Salesian College please contact the Headteacher.

2.8.13 Storage space on the school network is finite. Secure User Areas (attached to all staff & student accounts in the form of 'My Documents') are for work and educational use only. Users should keep non-work-related documents & files to a minimum. Users should not store any personal photos or videos on the network, nor should they use the school network to back up personal devices such as mobile phones/tablets. Access to non-work related files can and will be removed without warning at the discretion of IT Support based on storage requirements. Please contact IT Support for current guidance on appropriate storage of personal files.

2.8.14 Due to storage limitations, quotas are enforced on all user areas. These quotes are designed to ensure the fair distribution of ICT storage, taking into account the changing requirements of

users. It is every user's responsibility to ensure unnecessary files do not use up valuable storage space. If you require additional storage space, please contact IT Support via the Helpdesk.

2.8.15 Although it is not policy to routinely examine the content of individual user areas, the school reserves the right to monitor user areas at any time, for specific instances in which there is good cause for such monitoring or legal obligation to do so. Good cause shall include the need to fulfil legislative obligations, detect employee/student wrongdoing, protect the rights or property of the school, to protect the school ICT system security, to obtain essential business information after reasonable efforts have been made to contact the user or to comply with legal process.

2.9 **Wireless Access & Remote Access**

2.9.1 The school currently provides wireless facilities for all school-owned mobile devices, staff-owned mobile devices and where appropriate guest owned devices. All wireless access is provided at the discretion of IT Support and can be removed / revoked at any time.

2.9.2 Secure Wi-Fi access is provided for TSC staff members using the 'TSC Staff' Wi-Fi network (SSID). Staff may access this network using their school network username & password. Access to this network is strictly for staff-owned devices only, IT Support reserve the right to revoke device access at any time. Network access is monitored in real-time by IT Support.

2.9.3 Secure Wi-Fi access is provided for Sixth Form Students using the 'Thornleigh Sixth Form' Wi-Fi network (SSID). Sixth Form students may access the network using their school network username & password. Access to this network is strictly for Thornleigh Sixth Form student-owned devices. Further details of usage and restrictions of this network can be found in the Student IT Agreement document.

2.9.4 By connecting to the school Wi-Fi, users are agreeing to the terms of this document and any additional agreement required prior to connection. It is the responsibility of the individual to ensure their device software/OS is up-to-date, free from viruses and any other malicious software. IT Support reserves the right to revoke network access for any device deemed a threat to network security.

2.9.5 Designated users may access files and applications via the school's remote access facility. This is provided via a secure Remote Desktop System.

2.9.6 Access to the school Remote Desktop System is provided to all staff and select students at the discretion of IT Support & Senior Leadership Team. ICT Support reserve the right to remove access to the Remote Desktop System without prior notice when deemed necessary by the Headteacher on the advice from the Network Manager.

3. Data Security

3.1.1 Users must only access data held on the school's computer systems if they have been properly authorised to do so. Said data should only be used in the context of performing their designated role.

3.2 **Personal Data and the General Data Protection Regulation (GDPR)**

3.2.1 The school maintains a notification with the Information Commissioner's Office in compliance with the General Data Protection Regulation (GDPR). It is the responsibility of all school staff to ensure that personal data held and processed is within the terms of the school's data protection policy.

3.2.2 Under no circumstances should you disclose personal or other confidential information held on computer to unauthorised persons.

3.2.3 The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.

3.4 **Anti-Virus / Anti-Spam Protection**

3.4.1 Sophos Enterprise Anti-virus software is installed on all domain computers as standard and is updated regularly. Users are not permitted to disable or interfere with the running of anti-virus software.

3.4.2 Non-school software or data files intended to be run on school equipment by persons other than staff or students (including by not limited to school guests & contractors) must be checked for viruses before use. If you suspect that a virus has infected school ICT facilities immediately cease use and contact IT Support.

3.4.3 Un-encrypted files received by or sent by e-mail are checked for viruses automatically. Encrypted files may not always be scanned depending on their contents and file type. It is the user's responsibility to avoid accessing any suspect files and if received to alert IT Support to their presence.

3.4.4 Remote users are responsible for maintaining up-to-date anti-virus software on their own computers. Please contact IT Support if you require advice on protecting your personal device.

3.4.5 All user & email accounts provided to staff & students are the property of the school and are designed to assist in the process of teaching & learning. Users should have no expectation of privacy in any email sent or received, whether it is of a business or personal nature.

4. E-Mail

4.1 **Use and Responsibility**

4.1.1 Staff - the school email system is provided for the school's business purposes and academic support. Limited personal use of the email system is permitted, but not to a level that would influence the primary business purpose. The school will be held liable for any contractual arrangements entered into by email by members of staff if it is reasonable for the recipient to assume that such people are acting with authority (employer's vicarious liability). Such commitments should be avoided unless specifically authorised.

4.1.2 Students - the school's email system is provided to aid users with their studies. Personal use of the email system is permitted, but the account is only valid whilst you are a student at the school.

4.1.3 Users should not use school email when purchasing personal goods.

4.1.4 The email system costs the school time and money to maintain. It should be used judiciously in the same manner as other school resources such as telephones and photocopying.

4.1.5 School-wide email messages must be business related and of significant importance to all employees. Non-school email accounts should not be used for conducting school business unless in an emergency situation.

4.1.6 Communication with students through email should exclusively use the school E-Mail platform. Emails received from students using an alternative platform should be ignored and reported to the safeguarding lead/member of the Senior Leadership Team. Communications with students should remain strictly professional.

4.2 **Content**

4.2.1 Email messages must be treated like any other formal written communication. Improper statements in email can give rise to personal liability and liability for the school and can constitute a serious disciplinary matter.

4.2.2 Email messages to or from a school email address cannot be considered to be private or confidential to the individual.

4.2.3 Email can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.

4.2.4 Confidential or sensitive information should always be encrypted before being sent via email.

4.2.5 Thornleigh Salesian College email servers operate TLS 1.2 (Transport Layer Security) to ensure email is secured against interception when passing outside of the school network. Our email provider Gmail automatically encrypts all emails when leaving the school network.

4.2.6 Additional message-level email encryption is utilised by TSC senior leadership & administrative staff in the form of Egress Protect. Staff are required to use Egress Protect when sending sensitive data of any form via email to third parties outside of the school network. Recipient sign-up is required to use the service. If you are unsure about the use or application of Egress Protect please contact IT Support. Further information on Egress is available at https://supportcentre.egress.com

4.2.6

4.2.7 Email messages that may be intimidating, hostile or offensive on the basis of sex, race, colour, religion, national origin, sexual orientation or disability are strictly prohibited. It is never permissible to subject another person to public humiliation or ridicule; this is equally true via email. Any user found to have broken the above statute may have access to their school email account revoked without notice which may result in action via the school's Disciplinary Procedure.

4.2.8 Copyright law applies to email. Do not use e-mail to transmit or circulate copyrighted materials.

4.3 **Privacy**

4.3.1 Email messages to or from a school email address cannot be considered to be private or confidential. School emails will be regarded as the joint property of the school and the individual staff member or student.

4.3.2 Although it is not policy to routinely examine the content of individual emails, the school reserves the right to monitor messages, at any time, for specific instances in which there is good cause for such monitoring or legal obligation to do so. Good cause shall include the need to fulfil legislative obligations, detect employee/student wrongdoing, protect the rights or property of the school, to protect the school ICT system security, to obtain essential business information after reasonable efforts have been made to contact the mailbox user or to comply with legal process.

4.3.3 Emails are routinely scanned for the use of offensive language, inappropriate content / attachments, data protection breaches & spam content.

4.3.4 Messages sent or received may be copied and disclosed by the school for lawful purposes without prior notice. Requests for access/monitoring unless required by law will only be authorized by a member of SLT.

4.3.5 It is not permissible to access or to send email from another users account either directly or indirectly, unless directed to do so by Senior Leadership Team in the performance of your stated job role.

5. Cloud-based Learning Platforms

5.1 **Use and Responsibility**

5.1.1 Cloud-based software including Google Classroom and Class Charts are provided for the school's business purposes and academic support.

5.1.2 Communication using cloud-based virtual learning software must be treated like any other formal written communication. Improper statements can give rise to personal liability and liability for the school and can constitute a serious disciplinary matter.

5.1.3 Staff should ensure that any external resources shared within the virtual learning environment are appropriate for the audience.

5.2 **Privacy**

5.2.1 Confidential and sensitive information is available on cloud-based learning platforms and should only be accessed on a device which has the appropriate security and password protection to ensure non-authorised users do not have access to data.

5.2.2 Users should ensure that when data is accessed outside of the school network data is not accessible to family members and ensure that data remains confidential.

5.2.3 Although it is not policy to routinely examine the content of users online system activity, the school reserves the right to monitor activity, at any time, for specific instances in which there is good cause for such monitoring or legal obligation to do so. Good cause shall include the need to fulfil legislative obligations, detect employee/student wrongdoing, protect the rights or property of the school, to protect the school ICT system security, to obtain essential business information after reasonable efforts have been made to contact the mailbox user or to comply with legal process.

5.2.4 As 2.8.6 all mobile and tablet devices which are used to access school systems with sensitive data should have passcodes/biometrics.

6. Internet

6.1 **Internet**

6.1.1 All Internet usage from the school network is monitored and logged. Reporting on aggregate usage is performed on a regular basis. When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant user account. Such an

investigation may result in action via the school's Disciplinary Procedure and possibly criminal investigation.

6.1.2 Copyright and licensing conditions must be observed when downloading material or content from the internet or moving material on and off school network storage.

6.1.3 Once information is published on the world wide web it can be assumed it is freely accessible in the public domain. It is therefore critical that material of a proprietary or sensitive nature should not be published on unsecured public websites.

6.1.4 The school reserves the right to remove access to any site(s) which it feels may inhibit the primary business purpose of school.

6.1.5 The use of Social Media and its inherent dangers is outlined in the school Social Media Policy.

7. Private use, legislation and updates to this policy

7.1 **Private Use**

7.1.1 IT facilities are provided for the school's business and educational purposes and responsible personal use is therefore allowed provided there is no conflict with the interest or requirements of the school.

7.1.2 The school does not accept liability for any personal loss or damage incurred through using the IT facilities for private use.

7.2 **Legislation**

7.2.1 The following are a list of Acts that apply to the use of the school's IT facilities:

- Regulation of Investigatory Powers Act 2000
- Computers' Misuse Act 1990
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
- Race Relations Act 1976
- Disability Discrimination Act 1995
- Obscene Publications Act 1959
- Telecommunications Act 1984
- Protection of Children Act 1978
- Criminal Justice Act 1988
- General Data Protection Regulation 2018
- The Patents Act 1977
- Copyright, Designs and Patents Act 1988
- Defamation Act 1996
- Freedom of Information Act 2000
- Human Rights Act 1998

7.3 **Updates to this Policy**

7.3.1 In light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all staff will be made when updates are available. This policy will be reviewed ~~annually.~~every two years.

Student ICT Agreement – AUP supplemental

Students are permitted to use Thornleigh Salesian College ICT Facilities after agreeing to the following conditions:

1. I will use school ICT facilities, including the internet, e-mail, digital video, mobile devices, 3rd party services, virtual learning environment (Google Classroom) etc. for school purposes only.

2. I will not download or attempt to install software on school ICT Facilities.

3. I will only access the school network and 3rd party services using my own username and password supplied to me by the school.

4. I will follow the school's ICT Acceptable Use Policy and not reveal my passwords to anyone and change them regularly.

5. I will make sure that all ICT communications with other students, teachers or others are responsible and sensible.

6. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.

7. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.

8. I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring them into disrepute.

9. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community

10. I will respect the privacy and ownership of others' work on-line at all times.

11. I will not attempt to bypass the school internet filtering system in any way, regardless of what device I am using.

12. I understand that all my use of school ICT Facilities including Internet access and other related technologies is monitored and logged and can be made available on request to teachers.

13. I understand that these rules are designed to keep me safe and that if they are not followed, college sanctions will be applied and my parent/carer will be contacted.

14. I will not attempt to cause damage to the school infrastructure.

15. I will not attempt cyber-attacks.

Signature _____

Printed Name _____

Date _____

Guest and Staff ICT Agreement – AUP supplemental

Guests are permitted to use Thornleigh Salesian College ICT Facilities using the guest WIFI after agreeing to the following conditions:

1. I understand that I'm personally accountable for what I do online with school technology or using the school WIFI and infrastructure.

I will use school ICT facilities, including the internet, e-mail, digital video, mobile devices, 3rd party services, virtual learning environment (Google Classroom) etc. for school purposes only.

2. I will not download or attempt to install software on school ICT Facilities.

3. I will only access the school network and 3rd party services using my own username and password if supplied to me by the school.

4. I will follow the school's ICT Acceptable Use Policy and not reveal my passwords to anyone and change them regularly.

5. I will make sure that all ICT communications with other students, teachers or others are professional.

6. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of the senior leadership team.

7. I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring them into disrepute.

8. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community

9. I will respect the privacy and ownership of others' work on-line at all times.

10. I will not attempt to bypass the school internet filtering system in any way, regardless of what device I am using.

11. I understand that all my use of school ICT Facilities including Internet access and other related technologies is monitored and logged and can be made available on request.

12. I will not attempt to cause damage to the school infrastructure.

13. I will not attempt cyber-attacks.

14. I will only use the information, systems and equipment in line with our security and information management policies.

15. I will report any breach of this AUP to a member of the Senior Leadership Team

16. I am aware that I can use the 'Whistleblowing Policy', and raise a concern if it's believed that someone is misusing our information and technology.

17. I will ensure that computer devices connected to the school systems are locked / logged out of when not in use.

18. I understand that I have a legal responsibility to protect personal and sensitive information and adhere to the GDPR policy; social media policy; staff conduct policy.

19. I will not provide information in response to callers or emails whose identity I cannot verify.

Signature _____

Printed Name _____

Date _____