ACCEPTABLE USE OF IT POLICY

ACCEPTABLE USE OF IT POLICY

1. Rationale and Aims

All trainees are required to adhere to the Acceptable Use policies of the school in which they undertake an ITT placement. In addition, all trainees must familarise themselves with (and sign at the start of the course) the Sacred Heart SCITT policy as outlined below.

This policy is designed to protect staff, trainees and others from harm caused by the misuse of our IT systems, social media and our data.

Misuse of our IT systems includes both deliberate and inadvertent actions, both of which should be reported immediately to the SCITT Admin team and as appropriate the IT support team / senior team member responsible for IT systems.

The repercussions of misuse of our systems can be severe, for example, loss of staff/student data, or sensitive data being passed on to inappropriate third parties and phising/ransomware attacks with very significant financial consequences. Potential damage includes, but is not limited to: malware infection (e.g. computer viruses); legal and financial penalties for data leakage; and lost learning resulting from network downtime.

Everyone who works is responsible for the security of our IT systems and the data on them. As such, all staff and trainees must ensure they adhere to the guidelines in this policy at all times. Should anyone be unclear on the policy or how it impacts their role they should speak to the SCITT Manager or senior team member responsible for IT systems. An acceptable use agreement is included as an appendix to this policy which all staff and trainees must read and sign.

2. Definitions

“Users” are everyone who has access to any of Sacred Heart Catholic High School’s IT systems. This includes permanent staff and also temporary staff, contractors, agencies, consultants, suppliers, students and business partners, ITT students, governors and visitors.

“Systems” means all IT equipment that connects to the school network or accesses school applications. This includes equipment owned by the school or personal devices owned by individual members of staff and trainees. This includes, but is not limited to: desktop computers; laptops; smartphones; tablets; printers; data and voice networks; networked devices; software; electronically-stored data; portable data storage devices (memory sticks, external hard drives etc); third party networking services; telephone handsets; video conferencing systems; and all other similar items commonly understood to be covered by this term.

“Sensitive Data” means any personal information of students, trainees or staff including but not limited to: name; address; telephone number; date of birth; academic attainment and progress; photographs.

The “Data Protection Act (1998)” controls how personal information is used by organisations, businesses or the government. Everyone responsible for using data has to follow strict rules called ‘data protection principles’. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people’s data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

3. Use of IT Systems

Sacred Heart Catholic High School’s IT systems exist to support and enable learning in our school. A small amount of personal use is, in most cases, allowed. However, it must not be in any way detrimental to users own or their colleagues work, and nor should it result in any direct costs being borne by Sacred Heart Catholic High School. Personal use should be restricted where possible, to before/after school, break or lunchtimes. Sacred Heart Catholic High School trusts staff to be fair and sensible when judging what constitutes an acceptable level of personal use of the school’s IT systems. If staff are uncertain they should consult their head of department or a member of the IT support team.

Any information that is particularly sensitive or vulnerable (eg Contact details of students, PP, LAC information etc) must be encrypted and/or securely stored and/or password protected so that unauthorised access is prevented (or at least made extremely difficult). However this must be done in a way that does not prevent–or risk preventing–legitimate access by all properly-authorised parties.

Staff should be aware that any personal documents stored on the school network has the potential to be viewed by monitoring systems. This monitoring must be done to keep us in line with safeguarding requirements. Sacred Heart Catholic High School can monitor the use of its IT systems and the data on it at any time. This may include examination of the content stored within the email and data files of any user, and examination of the access history of any users.

Sacred Heart Catholic High School reserves the right to regularly audit networks and systems to ensure compliance with this policy and safeguarding.

4. Data Security

4.1 Sensitive Information:

Wherever possible users should ensure that files which contain personal details of students, trainees or staff remain on the school network or Office 365 system, and are not transferred to other systems, or stored on personal devices of any kind. This is to ensure the security and integrity of the data, and also ensures that regular backups are taken which can be recovered when necessary. If access to such files is required while away from school, staff should use the Office 365 service or the ‘Remote Desktop’ facility.

Information stored on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, therefore special care should be exercised with these devices: sensitive information should be stored in encrypted folders only, or password protected. Users will be held responsible for the consequences of the theft, or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it. If sensitive information must be taken out of school on personal devices, it is up to the individual to ensure that the sensitive information is appropriately protected. This information must be deleted/copied back onto the school's IT system at the earliest opportunity. The IT support team will be happy to assist any member of staff who needs help in this area.

Users should not display sensitive information contained in PARS / SIMS or any other IT system using data projectors. This is to ensure other students in the class do not see personal information of other students. The freeze button on the projector remote should be used when the projector is on, and staff need to use PARS / SIMS, or access any other sensitive information.

Staff should be aware that any comments about students that are recorded in PARS can be viewed by their parents using the Insight system, and so are advised to always ensure such comments are appropriate.

4.2 Password Security:

Users must keep passwords secure and not allow others to access their accounts. Secure passwords contain a random mixture of lower and uppercase letters, numbers and punctuation. Users will be prompted to change their password every 90 days.

4.2 Device Security:

Users who are supplied with computer equipment by Sacred Heart Catholic High School are responsible for the safety and care of that equipment, and the security of software and data stored on it and on other Sacred Heart Catholic High School systems that they can access remotely using this device.

All workstations (desktops and laptops) should be manually locked by the responsible user whenever leaving the machine unattended for short periods, and users must log out when they are leaving the machine unattended for longer periods. All workstations should be shut down at the end of the day.

4.3 System Security:

The IT support team are responsible for ensuring that the IT systems are properly protected at all times against known threats and vulnerabilities, as far as is reasonably practicable in our school.

All users have a duty of care and therefore must, at all times, guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into Sacred Heart Catholic High School's systems by whatever means and must report any actual or suspected malware infection immediately to the IT support team.

5. Unacceptable Use

All staff should use their own judgement regarding what is unacceptable use of Sacred Heart Catholic High School's systems. However, the activities below are provided as examples of unacceptable use, although the list is not exhaustive:

- All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.

- All activities detrimental to the success of Sacred Heart Catholic High School as well as defamation of the school.

- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the school. These include activities that slow down the computer network (e.g., streaming video, playing networked video games).

- All activities that are inappropriate for Sacred Heart Catholic High School to be associated with and/or are detrimental to the schools' reputation. This includes pornography, gambling, inciting hate, bullying and harassment. (See E-Safety policy).

- Circumventing the IT security systems and protocols which Sacred Heart Catholic High School has put in place.

- All personal activities which result in costs being borne by the school

Should any member of staff need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from the IT systems manager before proceeding. (For example, needing to access social media accounts following a pastoral issue.)

6. Bring Your Own Device (BYOD)

Sacred Heart Catholic School provides a wireless network which allows staff, trainees, sixth form and visitors access to the school's broadband internet service. There are four wireless networks available for specific users as described below:

SH-SCHOOL	For use on **school based equipment only**, and must not be used with personal devices. The wireless key will not be shared with any user other than IT support staff.
SH-STAFF	For teachers, ITT trainees and support staff only, accessed and authenticated with their usual network username and password (no wireless key is necessary)
SH-SIXTH	For sixth form students only, accessed and authenticated with network username and password (no wireless key is necessary)
SH-GUEST	For external visitors only. Authenticated with a wireless key held by admin staff in the school's front office. This wireless key will be changed regularly for security purposes.

Details of how to access each wireless network should not be passed on, other than to those stated in the table above.

Sacred Heart Catholic High School's BYOD service is only for the purposes of work related activities which need internet access, including:

- Any work-related internet activity. This access is filtered using the school's 'Smoothwall' filtering system.
- Email services
- Data held on PARS / SIMS / other administrative systems
- Office 365

The service does not allow any user access to:

- Personal network user areas stored on site
- Shared network areas stored on site
- Network printers
- Any other network resource, other than those accessed via the internet service

Staff & ITT Trainee Acceptable Use Agreement

This acceptable use agreement covers the use of all systems in Sacred Heart Catholic High School as defined in the 'Acceptable Use of IT Policy'.

- I will only use the IT systems at Sacred Heart Catholic High School for professional purposes
- I will ensure that all sensitive data is stored only on systems within Sacred Heart Catholic High School, its Remote Access System, or the Office 365 secure cloud storage system.
- I will ensure any personal digital devices used by me do not contain sensitive data relating to students or staff of Sacred Heart Catholic High School
- I will ensure any personal devices used in school have adequate antivirus/spyware software installed to prevent infecting school based equipment via the network
- I agree that any sensitive data I may need to use for professional purposes while away from Sacred Heart Catholic High School will be adequately protected using encryption methods and/or password protection
- I agree to use a secure password to access the IT systems at Sacred Heart Catholic High School, and to change this every 90 days
- I will be responsible for the safety and care of any IT equipment loaned to me by Sacred Heart Catholic High School, and the security of any data stored on it
- I will lock all desktop / laptop devices while away for short periods
- I will log off all desktop / laptop devices while away for longer periods, or when another member of staff may need to log on
- I will shut down all desktop / laptop devices at the end of the day
- I will take all reasonable steps to ensure any personal digital devices which connect to the IT systems at Sacred Heart Catholic High School are protected again malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors)
- I will not use the IT systems at Sacred Heart Catholic High School for the activities stated below:
    - All illegal activities, and activities that contravene data protection regulations.
    - All activities detrimental to the success of Sacred Heart Catholic High School as well as defamation of the school.
    - All activities for personal benefit only that have a negative impact on the day-to-day functioning of the school.
    - All activities that are inappropriate for Sacred Heart Catholic High School to be associated with and/or are detrimental to the schools' reputation.
    - Any activity which would circumvent the IT security systems and protocols which Sacred Heart Catholic High School has put in place.

Staff & ITT Trainee Acceptable Use Agreement

ACCEPTABLE USE OF IT POLICY

I confirm that I have read and are aware of the implications and regulations of use as stated within the Acceptable User policy

ITT Trainee Name: ……..

Signature: ……

Date: ……

If there are any issues which would prevent a trainee from signing this agreement, they should speak to the SCITT Manager in the first instance.

Please hand this copy to SCITT Manager