St Faith's School Policies
Information Technology Acceptable Use Policy

Contents

1. Introduction

The Information Technology Acceptable Use Policy (ITAUP) has been drawn up to set out the School's conditions of use of the School's Information Technology resources by members of the school community. This policy takes into account applicable data protection law (principally the UK GDPR and Data Protection Act 2018), applicable anti-radicalisation laws[1] and best practice in safeguarding[2]. Its purpose is to set out the principles and guidance, which you must bear in mind at all times and also give you some rules, which you must follow. As with every set of rules an occasion could arise which will fall outside them. In a case like this, you should refer to the principles in this policy and if necessary contact the IT Manager/Team for clarification.

This policy applies to all members of the school community who use school IT systems, as a condition of access. Access to school systems is not intended to confer any status of employment on any contractors.

2. Related Policies

St Faith's adopts the following policies that relate to the ITAUP:

- Artificial Intelligence Policy
- Anti-bullying Policy
- CCTV Policy
- Data Breach Policy
- Data Protection Policy
- Data Retention Policy
- Information Security Policy
- Pastoral Behaviour and Discipline Policy
- Personal Device Policy
- Safeguarding and Child Protection Policy
- School Privacy Notices
- Staff Handbook ad Code of Conduct
- Taking, Storing and Using Images of Children Policy
- Whistleblowing Policy and Procedure

All School policy documents are held on the server and may be accessed via SharePoint at this link.

3. Principles of online behaviour

As a member of the school community you should follow these principles in all of your online activities:

3.1. Respectful communication

The school cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.

1 Prevent Duty Guidance for England and Wales (September 2023)
2 The Independent School Standards Regulations (April 2019), Keeping children safe in education (September 2023), Working Together to Safeguard Children (December 2023), DfE, Generative artificial intelligence in education – Departmental statement (March 2023)

3.2. Content Integrity

Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).

3.3. Privacy Protection

Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.

3.4. Intellectual Property Respect

Do not access or share material that infringes copyright, and do not claim the work of others as your own.

3.5. Cybersecurity Vigilance

Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.

Please follow any guidance and complete any training provided by the IT Team in relation to Cybersecurity.

If any Cyber related incidents occur please report to the IT Manager and/or team immediately.

3.6. Professional Boundaries

Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

4. Use of School's Property

Any device belonging to the School should treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the School's IT Team.

5. Passwords

Passwords protect the school's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

As a rule of thumb, a strong password is:

- At least 12 characters long but 14 or more is better.
- A combination of uppercase letters, lowercase letters, numbers, and special characters.
- Significantly different from your previous passwords.

Easy for you to remember but difficult for others to guess. Consider using a memorable phrase like "6MonkeysRLooking^".

6. School Systems

School IT systems encompass a range of technologies and services that support the school in various aspects. Here are some key components of school IT systems:

6.1. IT for Teaching and Learning

- *Educational Software:* Tools and applications used for teaching, learning, and student engagement. These include interactive learning platforms, virtual labs, and educational games.
- *Display and Presentation Equipment:* Projectors, interactive whiteboards, and audiovisual systems that enhance classroom teaching.
- *Devices for Teachers and Pupils:* Laptops, tablets, and other devices used by educators and students for accessing digital content and collaborating.

6.2. IT for Administration

- *Back Office Software*: Systems for managing administrative tasks such as HR, finance, payroll, and facilities management.
- *Management Information Systems (MIS)*: Software that handles student records, attendance, timetabling, and reporting.
- *Data Analysis Tools:* Tools for analysing student performance data and identifying trends.
- *Fundraising and Marketing Software*: Solutions to manage fundraising campaigns and promote the school.

6.3. IT for Development

- *Digital Leadership and Governance:* Strategies and policies for effective technology adoption and management.
- *Network Infrastructure:* Ensuring reliable connectivity, including wired and wireless networks.
- *Security Measures:* Protecting data, systems, and users from cyber threats.
- *Digital Accessibility:* Ensuring that digital resources are accessible to all, including students with disabilities.

All official school business must be conducted on school systems, and it is not permissible to use personal email accounts for school business. The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education only. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts.

The contents of our IT resources and communications systems are the property of St Faith's. Therefore, staff and pupils should have no expectation of privacy in any email, file, data, document, facsimile, telephone conversation or social media post. There should also be no expectation of privacy in any other kind of information or communication transmitted to, received, printed from, stored or recorded on our electronic information and communications systems.

We reserve the right to monitor, intercept and review, without further notice, all activities using our IT resources and communications systems, including but not limited to social media postings and activities and internet sites visited. This allows us to ensure that our resources and communication systems are being used for legitimate business, safeguarding, conduct and performance purposes and to ensure that our network policy and principles are being complied with.

The School reserves the right to examine or delete any files that may be held on its computer files.

7. Rules for using the school's IT systems

Whenever you use the school's IT systems you should follow these rules:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed and/or used on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install or download software on, or otherwise alter, school IT systems and devices.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.
- For any items that are deemed suspicious or unacceptable please report to the IT Manager immediately.

8. Use of personal devices or accounts and working remotely

Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer or cloud– must be registered and approved by the School's IT Team.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies.

9. Monitoring and access

Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined under such circumstances following the School's Pastoral, Behaviour and Discipline Policy.

10. Social Media/Social Networks

Social media refers to a form of **mass media communications on the Internet**. It encompasses websites and applications that enable users to create and share content or participate in social networking. Social networking is defined as the use of dedicated websites and applications to interact with other users, or to find people with similar interests to one's own. While social networking and social media overlap, social networking focuses on users building communities among themselves, while social media emphasizes using platforms to build an audience.[3]

A separate policy exists to inform and regulate the use of social media at St Faith's for both business and personal purposes, whether during School/working hours or otherwise. This policy applies regardless of

3 Britannica, The Editors of Encyclopaedia. "social media". Encyclopaedia Britannica, 11 Jun. 2024, https://www.britannica.com/topic/social-media. Accessed 12 June 2024.

whether the social media is accessed using our IT facilities and equipment or other IT equipment (including IT equipment belonging to staff). In any event, staff may not use their work email address for any personal use of social media.

11. Tracking Devices and Technology

The school is not responsible for individual settings on personal devices, nor for the use of tracking apps / devices for purely personal and domestic purposes.

Use of this technology in the context of school activities is not specifically encouraged but if parents do plan to use it then they should be aware of potential third party privacy considerations and only use it for domestic / personal purposes in respect of their own child and/or their or their child's belongings.

That said, the school is aware that there may be instances where such technology – whether, for example, for security of belongings or for parents' peace of mind as to children's whereabouts – can be used appropriately and proportionately. We would encourage parents / pupils to raise any such requests with us, for example in advance of a trip, so that we can discuss appropriate usage.

12. Retention of digital data

Staff and pupils should also be aware that data is collected and handled to ensure the School operates effectively. The School's Data Protection Policy sets out its responsibilities under the UK GDPR, and data storage is governed by the Data Retention Policy.

Electronic information will be retained for at least the period specified in the retention schedule at Annex A of the Data Retention Policy. When managing records, the School will adhere to the standard retention times listed within that schedule.

If you consider that reasons exist for the Data Retention protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the IT Manager.

13. Breach reporting

The school must take steps to ensure data breaches are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, e.g. through the use of malware;
- application of the wrong privacy settings to online systems;

- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the ICO[4] without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If you become aware of a breach of this policy you should report it to the School's Data Compliance Officer[5].

Failure to follow the principles and/or rules stated above and on related policies may result in the school restricting your access to school IT systems and lead to disciplinary action being taken.

14. Acceptance of this policy

14.1. Members of Staff

To ensure compliance with the ITAUP, the following procedure is implemented for all staff members:

Upon acceptance of employment, staff members are required to demonstrate their understanding and agreement to the Acceptable Use Policy by completing and signing the Declaration of Acceptance (Appendix 1).

On first day of work, Staff members will undergo an IT induction and training to familiarize themselves with the IT systems and policies.

In the event of any amendments to the policy, staff will be notified through the We Are Every System, where they will be required to acknowledge the changes.

14.2. Pupils

- **Pre-Prep:** Parents are required to sign the agreement on the My School Portal. Upon completion, a notification is automatically sent to the IT Manager to confirm the acknowledgment.
- **Prep:** The agreement will be reviewed by the Head of Computing during the first computing lesson of the academic year. Following the review, pupils are expected to sign the agreement. A copy of the signed agreement should then be forwarded to the IT Manager.

14.3. Guests

- **When IT access is required:** The agreement is dispatched to the relevant parties. It is imperative that the agreement is signed to grant IT access.
- **Upon signing in to the school site:** The agreement can be obtained from the **InVentry system**. This ensures that all individuals signing into the school site have agreed to the Acceptable Use Policy.

R P BRENT MBE
Bursar

[4] Information Commissioner's Office
[5] The School Compliance Officer.

Appendix 1: Declaration of Agreement for IT Acceptable Use Policy

Member of Staff

I, the undersigned, hereby acknowledge that I have read and understood St Faith's IT Acceptable Use Policy. I agree to adhere to the principles and guidelines set forth within the policy and understand that failure to comply may result in disciplinary action, up to and including termination of employment.

Name:_____
Signature:_____ Date:_____

Parents of Pupils (Pre-Prep):

As the parent or legal guardian of the child named below, I confirm that I have reviewed the IT Acceptable Use Policy with my child and understand the importance of adhering to its terms. I agree to support the school in enforcing the policy and ensuring my child's compliance.

Name of Parent/ Legal Guardian:_____
Name of Pupil _____
Signature:_____ Date:_____

Pupils (Prep)

My name is: _____

I promise to follow the rules when I use computers and the internet at school. I will:

- Be kind and respectful to others online.
- Keep my personal information private.
- Tell a teacher if something online makes me feel uncomfortable or if I see someone not following the IT rules.
- Only use the internet and school devices for schoolwork and learning.
- Do not share my password with anyone..
- Do not attempt to download or install anything on school devices.

I understand that these rules are here to keep me and my friends safe and that not following them might mean I can't use school devices for an agreed period.

My signature (that means my name written by me):_____

Today's date:_____

Guest
I acknowledge that I have been provided with a copy of the IT Acceptable Use Policy. I understand that as a guest, I am required to follow the policy while accessing IT resources on the institution's premises. I agree to use these resources responsibly and in accordance with the policy.

Signature:_____ Date:_____

Appendix 2: Glossary

Term	Definition
AI	Artificial Intelligence (AI) is defined as the theory and development of computer systems able to perform tasks that normally require human intelligence. These tasks include visual perception, speech recognition, decision-making, and translation between language.
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Internet	The Internet is a global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Network	A computer network is defined as a set of computers that are connected with one another for the purpose of communicating data electronically
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate)