



Acceptable Use of IT Policy

Role Responsible:	Assistant Principal (Director of Finance & Resources)
Written by:	Head of IT Infrastructure & Network Services
Date approved:	17 April 2023
Approved by:	SLT
Publication:	Google Shared Drive – Itchen Staff – Staff Policies
Review cycle:	Annually
Next Review Date:	April 2024

Contents

Revision History	2
Contents	3
Introduction	4
Scope	4
Acceptable Use of IT	5
Keeping Your IT Account Secure	5
Safeguarding of Information	6
Compliance with Data Protection	6
Behaviour	7
Monitoring	8
Further Information	8

Introduction

This policy is intended to ensure that Itchen Sixth Form College's IT systems are used safely, lawfully and equitably.

This Acceptable Use Policy is intended to provide a framework for such use of the College's IT resources. It applies to all computing, telecommunication, and networking facilities provided at the College. This policy should be interpreted so as to encompass new and developing technologies and uses, which may not be explicitly referred to.

This Acceptable Use Policy is taken to include the [JANET Acceptable Use Policy](#) and the [JANET Security Policy](#) published by JISC. Members of the College and all other users of the College's facilities are bound by the provisions of these policies in addition to this Acceptable Use Policy. They are also bound by such other policies as are published via the College on the College Intranet. It is the responsibility of all users of Itchen College's IT systems and services to read and understand this policy.

Scope

This policy applies to anyone using College IT systems (hardware, software, data, network access, telephony, online cloud-based services, services provided by licensed third parties or using College IT credentials) including staff, students, guests, and third party individuals who have been given access for specific purposes. It is the responsibility of all users of the College's IT systems to read, understand and comply with this policy and any additional policies related to their activities, including other relevant IT policies.

This policy is issued under the authority of the Senior Leadership Team. Responsibility for their interpretation and enforcement is delegated to IT Services.

You must comply with any reasonable written or verbal instructions issued by IT Services staff with delegated authority in support of this policy. If you feel that any such instructions are unreasonable or are not in support of this policy, you may appeal to the IT Network Manager.

Acceptable Use of IT

College IT resources are provided primarily to support teaching, learning, and business functions. IT systems are also provided to students to enhance their wider experience at Itchen College.

College IT systems may be accessed via College owned devices or via personally owned devices, however this policy remains applicable regardless of the ownership of the device used. Personally owned devices whether owned by students or staff must be maintained with up to date anti-virus software (where appropriate), system patches and kept secure in accordance with the College Bring Your Own Device Policy. Devices provided to staff or students by the College for their personal use must also be kept secure in a similar manner.

Use of facilities for personal activities is permitted, provided that it does not infringe the law or College policies, does not interfere with others' valid use and, for staff, is not done inappropriately during their working hours. However, this is a privilege that may be withdrawn by the IT Network Manager, at any point, if such use is not in accordance with this policy.

Using College owned or managed services for commercial work or business trading, that is being undertaken on a personal basis, solely for personal gain and not through College channels, is not permitted.

College email addresses and associated systems, must be used for all official College business, in order to facilitate auditability and record keeping. All staff and students of the College must regularly read their College email. College email addresses are not be used for personal use in lieu of a personal email address, for example, registering on ecommerce websites, subscribing to mailing lists, etc.

You must abide by the policies and terms & conditions applicable to any other organisation whose services you access. When using Itchen College IT Services from another institution via eduroam, you are subject to both Itchen College's requirements and those of the institution where you are accessing services.

Users must adhere to any licence conditions when using software procured by the College.

Further details of what constitutes acceptable and unacceptable use is provided in the subsequent sections of this policy.

Keeping Your IT Account Secure

You must take all reasonable precautions to safeguard your username, password, and any other IT credentials issued to you. Advice is available on the choice of . You must not allow anyone else to use your IT account. No-one has the authority to ask you for your password, and you must not disclose it to anyone, including the IT Helpdesk.

You must not attempt to obtain or use anyone else's credentials.

You must not impersonate someone else or otherwise disguise your identity when using the IT systems.

Safeguarding of Information

You must take all reasonable steps to safeguard any information you have access to in accordance with the law (Data Protection Act).

You must not infringe copyright, or break the terms of licences for software or other material. Copyright applies to all text, pictures, video and sound, including those sent by email or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded, incorporated into any college documents or web pages, or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

You also have a responsibility to ensure College data is securely maintained and is available for backup:

- You must not store any files on the local drive of a computer (this excludes the normal functioning of the installed operating system or other authorised systems such as the Movies/Projects folder setup for Media). Instead, users must save data on the provided network storage. Files that are stored “locally” will not be backed up
- The use of External media, such as external hard drives, SD cards and USB sticks is discouraged. Wherever possible, data must be stored on College systems or approved Cloud-based service.
- Where the use of External media is unavoidable, such media must not be used to store sensitive, college or personal identifiable information
- Cloud-based services other than those provided by the College, such as Google’s G Suite for Education, must not be used to store College data.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory.

All communications and files created using the College systems remain the property of the College. The College reserves the right to keep copies of users files and to disclose them to law enforcement or other legal authorities without the consent of the user. The College reserves the right to use the content of any employee email or file in any disciplinary process.

Compliance with Data Protection

The college is committed, as a data controller and data processor, to treating all personal data fairly and lawfully in line with the General Data Protection Regulation. This includes the requirement to keep personal data up-to-date, and to handle it securely and to keep it for no longer than is necessary

All users are required to comply with the college data protection policy and requirements. Your personal responsibility is expected to align with these college obligations.

Your attention is drawn to the separate Itchen College Data Protection Policy which requires you as an individual to process data in compliance with all aspects of the Data Protection Act

and this applies equally to processing of data which takes place on either college owned devices or personal devices.

Employees of the College have a responsibility to ensure that data is stored, transferred, handled and destroyed in accordance with the college records management plan. This requirement includes college information originating from your own device.

Employees are also required to assist the college in complying with subject access and FOI requests for information and you may be required to search your device and to provide the information requested to the college.

Behaviour

The conduct of staff and students when using the College's IT systems should always be in line with the College Values, including the use of online and social network platforms (staff should also refer to the Staff Professional Code of Conduct regarding Social Media and Networking). When using College IT systems you must not:

- Generate, install, bring into College, or download material that could cause offence to others, be detrimental to the well being of others, or bring the College into disrepute
- Use the IT systems in a way that interferes with others' valid use of them
- Not to transmit material that infringes the copyright of another person, or their intellectual property rights;
- View, store or print pornographic images or video
- The retention or propagation of sites or media which are specifically designed to promote terrorism or which are directly linked to a proscribed terrorist organisation, except in the course of recognised research or teaching that is permitted under UK and international law
- Use the College's internet facilities to download entertainment software, including games
- Send spam or unsolicited bulk messages to any users whether internal or external, or use College email groups other than for legitimate purposes related to College activities
- Deliberately or recklessly consume excessive IT resources such as network storage space, processing power, bandwidth, or consumables
- Undertake any activity that risks the security, integrity, performance or reliability of college computers, software, data and other stored information
- Deliberately or recklessly introduce malware or viruses
- Attempt to circumvent IT security measures or internet filtering, which will constitute gross misconduct
- Not to tamper with, move or disconnect any IT systems, equipment or associated peripherals unless explicitly authorised to do so by the IT Network Manager or his delegate
- Not to copy software from the College IT systems, nor install software on to the College IT systems (including local hard drives and personal network space) without the express permission of the IT Network Manager or his delegate

Monitoring

Itchen College records and monitors the use of its IT systems, under the Regulation of Investigatory Power Act (2000) for the purposes of:

- The effective and efficient planning and operation of the IT systems
- Investigation, detection and prevention of infringement of the law, this policy or other College policies
- Investigation of alleged misconduct by staff or students
- Monitoring of staff and student use of systems for safeguarding to prevent potential harm to self or others.

Users consent to responsible College IT Services staff monitoring their use of IT systems and investigating their files and activities, this may involve monitoring internet access, emails, and the remote monitoring of screens.

The College's internet access incorporates a content filtering system to block inappropriate websites and applications. The content filter used on the College network aims to achieve the following:

- Access to inappropriate sites is blocked
- The content of web pages or web searches is dynamically filtered for inappropriate or suspicious keywords in accordance with the College's eSafety Policy
- Records of blocked internet sites by students and staff are logged
- Records of inappropriate or suspicious search engine keywords categorised as adult and profanity, extremist, and self harm are logged

Accessing a site denied by the content filter or using inappropriate or suspicious search engine keywords will result in a report being generated and passed onto the IT Network Manager.

Itchen College will comply with lawful requests for information from government and law enforcement agencies.

Access to home drives, email, and/or individual usage information will not normally be given to another member of staff unless authorised by the IT Network Manager, or nominee, who will use their discretion, normally in consultation with the Assistant Principal (Finance and Resources), line manager or other senior staff.

The standards set out in this Policy are designed to minimise the risk of incurring liability in relation to staff or student usage of IT systems. The College may take disciplinary action against anyone who breaches any of the requirements contained in this Policy, which may include summary dismissal for those committing acts of gross misconduct.

Further Information

Within this document the term “College IT Systems” relates to computers, associated equipment, peripherals and to data networks, both internal and external, which are the property of the College or the property of a supplier to the College.

Users must comply with all relevant legislation and note that many acts of parliament apply to the use of computer equipment, including:

- General Data Protection Regulation (GDPR)
- Malicious Communications Act 1988
- Computer Misuse Act 1990
- Communications Act 2003
- Regulation of Investigatory Powers Act 2000
- Investigatory Powers Act 2016
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Counter-Terrorism and Security Act (2015)