Information Communications Technology Acceptable Usage Policy for Students and Staff

This Policy sets the 'ground rules' for what Spurgeon's College regards as acceptable use of Information Communications Technology (ICT) facilities. The Policy applies to all staff, students and authorised users of our ICT facilities.

Introduction

The vast majority of students and staff of Spurgeon's College are conscientious users of ICT. However, it is possible that a small minority of individuals occasionally challenge our expected norms of acceptable use, either deliberately or unintentionally. The purpose of this Policy is to provide guidance on what constitutes 'acceptable use' and 'unacceptable use'.

Responsibility

The Director of Operations has ultimate responsibility for the updating and implementation of this acceptable usage policy. New staff, students and volunteers and authorised users will be made aware of this policy as part of their induction process.

The College accepts no responsibility for the malfunctioning of any ICT facility or part thereof, whether hardware, software or other.

Legislation

Users must comply with all relevant external guidelines, laws, policies and procedures which affect the use of the College's ICT facilities, including:

- Computer Misuse Act 1990
- Data Protection Act 1998
- Copyright, Designs & Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- Counter-Terrorism and Security Act 2015

Scope of this policy

The principles and obligations described in this Policy apply to all users of the College's ICT facilities, including staff, students and third parties having access to College ICT facilities in whatever form. College ICT facilities include, but are not restricted to:

- network infrastructure, including the physical infrastructure whether cable or

wireless, network servers, firewalls, switches and routers;

- network services, including internet access, web services, broadband, email, wireless, messaging, network storage, telephony and
- fax services, CCTV, door and access control;
- computing hardware, both fixed and portable, including personal computers, workstations, laptops, tablets, mobile devices, smart phones, servers, printers, scanners, disc drives, monitors, keyboards and pointing devices;
- software and databases, including applications, web applications, virtual learning environments, video-conferencing, language laboratories, software tools, e-library services, electronic journals and eBooks;
- social networking media or services provided by the College.

Control of ICT facilities and monitoring

Subject to UK legislation[1], the College reserves the right to monitor, scan or otherwise probe its ICT facilities, systems and networks, in order to detect potential problems, investigate security issues and maintain an efficient service. The reasons for undertaking such monitoring include:

- investigating or detecting unauthorised use of ICT facilities;
- detecting security vulnerabilities;
- preventing or detecting criminal activities;
- ensuring compliance with College policies;
- ensuring effective system operation.

The College also reserves the right to inspect any items of computer equipment connected to the network. Access to the College's network will be removed if a user is deemed to be breaching College policy or otherwise interfering with the operation of the network.

Charging

The college reserves the right to charge users for acceptable use of the College ICT facilities (e.g. printing). Where such charges are deemed necessary will be outlined elsewhere.

All loss or damage of ICT equipment must be reported to the Director of Operations at the earliest opportunity. The College reserves the right to charge users for the cost, as determined by the Director of Operations, of remedying any damage (accidental or otherwise) they cause to College ICT equipment or facilities.

Acceptable use

College ICT facilities are provided by the College to authorised users for College purposes – primarily to support teaching, learning and research and to support professional and administrative activities. Users of College ICT facilities must seek to use such facilities in a way which is deemed acceptable by the college:

[1]Any monitoring will take place within the terms permitted under the Regulation of Investigatory Powers Act (RIP) 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

1. All internet access is filtered by our internet provider (London Grid for Learning) to block inappropriate material. Users should not attempt to circumvent this filtering process. If a user considers a website has beeninappropriately blocked please see the Director of Operations who will be able to unblock it.
2. In certain teaching or research activities, staff or students might need to access material which falls outside of the acceptable use for the purposes of legitimate study. In such cases where unusual access is required, this should be agreed by the college Principal and may need authorisation under the College's security sensitive research policy.
3. Users must take every precaution to avoid damage to equipment caused by eating or drinking in its vicinity.
4. Users must adhere to the terms and conditions of all licence agreements relating to ICT facilities which they use including software, equipment, services documentation and other goods.
5. Consumables including stationery must be used for the purpose for which they are supplied and their consumption should be minimised as far as is reasonably possible. Where printing facilities are provided without charge, it is expected that a maximum of two copies of a document be printed and that any additional copies be made by photocopying.

The College allows staff and students reasonable personal use of ICT. It is important to understand what constitutes reasonable use – both in terms of scale and activity. For example, reasonable personal use might include:

1. Personal electronic communications and recreational use of internet services, (e.g. email, instant messaging, micro blogging, online shopping and web surfing). These are permitted, provided that these activities remain within expected norms of behaviour and are not excessive in that they do not interfere with one's duties, or the work of others.
2. Storing non-College work related information on College systems – for example, eBooks, music, home videos, photography. Such storage must not be excessive and it must not infringe copyright and data privacy legislation. Non-College work information may be removed at any point without warning and it is the users responsibility to keep a separate backup of this information. The College cannot be held responsible for the security, loss, damage, backup or recovery of non-work related information.
3. Occasional and limited personal use of College ICT facilities by staff is permitted, but such use is a privilege and not an automatic right. Personal use of College ICT facilities must not hinder or interfere with any contractual or professional duties.
4. Personal use of College ICT facilities must not prevent the legitimate use of these facilities by others for the purposes of supporting their learning, teaching and research or prevent the use of the facilities for College administrative activities.

Unacceptable use

Unacceptable use of the College's ICT equipment, services or facilities includes:

- illegal and unlawful activity;

- unauthorised use of services and facilities;
- breach of copyright;
- compromising security;
- causing disruption and mischief;
- negatively affecting the reputation of the College;
- activities likely to draw people into terrorism or extremist ideologies[2];
- misuse of electronic messaging and social media;
- carrying out unauthorised personal legal and business transactions.

Unacceptable use extends to staff or student behaviour which may impact upon the College by virtue of the association between an individual and the College.
A non-exhaustive list of examples of unacceptable use of College ICT facilities is:

a) Illegal or unlawful

Several pieces of UK legislation define acceptable computer use, chief amongst these being the Computer Misuse Act 1990. This Act created offences, including using another person's username or identifier (ID) and password without proper authority to access (or attempt to access) data; to alter, delete, copy or move a program or data, or to impersonate another person using email, online chat, web or other services. Subsequent exploration may be illegal if it leads to entry to parts of the system for which access is not authorised.

1. Publishing material or making statements which the College may deem to be advocating illegal activity, or threatening, or harassing, or defamatory, or bullying or disparaging of others, or abusive, or libellous, or slanderous, or indecent, or obscene, or offensive or otherwise causing annoyance, inconvenience or needless anxiety.
2. All activities that are illegal or in conflict with College policies, procedures, processes and regulations.
3. All actions which breach regulations and policies applied to the College by external bodies e.g. the providers of electronic journals etc.
4. Using College ICT facilities for unauthorised personal, commercial or financial gain, or for unauthorised personal legal and business transactions.
5. Committing the College to a contract unless officially authorised to do so.
6. All activities of a nature that compete with the College in business unless specifically authorised.
7. All activities that waste staff effort, time or network resources, or deny service to other users.
8. Publishing material or making statements which unlawfully discriminate or which promotes unlawful discrimination.
9. Any activity which is in breach of the College's Data Protection Policy.
10. Staff must not disclose restricted information relating to his/her employment at the College.

    Any activity which promotes or encourages acts of terrorism or attempts to draw people into terrorism, terrorist groups, terrorist activities or extremist ideologies.

[2] This is a duty under section 26 of the Counter-Terrorism and Security Act 2015.

Note: The UK government has defined extremism as: ‘vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces’.

b) Indecent or offensive

The Obscene Publications Act 1959 and 1964 makes it illegal to publish material that tends to deprave and corrupt those viewing it. Under the 1964 Act, it is an offence to possess obscene material with an intention to publish for gain. So no attempt to publish is required for the crime to have been committed. All of this then applies equally to the electronic world.

College ICT facilities must not be used for access, creation, modification, storage, download, hosting or transmission of material that could be considered offensive, obscene, pornographic, or otherwise inappropriate. College ICT facilities must not be used for placing direct or indirect links to websites which publish or host pornographic, offensive or inappropriate material.

c) Unauthorised access

It is an offence to use or access another person’s account without proper authority. Even if the initial access is authorised, subsequent exploration may be illegal if it leads to entry to parts of the system for which access is not authorised.

1. Unauthorised access (or attempted unauthorised access) to facilities or services provided by the College network or accessible from the College network is not permitted.
2. Allowing, inciting, encouraging or enabling others to gain or attempt to gain unauthorised access to the College’s computer facilities; or to carry out unauthorised modification to the College’s computer facilities, is not permitted.
3. Registering any domain name which includes the name of the Spurgeon’s College or any similar name which may mislead the public into believing that the domain name refers to the College is not permitted.
4. Unauthorised transmission, distribution, discussion or disclosure (e.g. on email or similar media including social media sites) to a third party of any restricted data (i.e. sensitive, confidential or commercially sensitive information) is not permitted.

d) Breach of copyright and intellectual property

Copyright gives the creators of certain kinds of material rights to control the ways their material can be used. These rights start as soon as the material is recorded in writing or in any other way. Copyright applies to any medium. This means that you must not reproduce copyright protected work in another medium without permission.

1. College ICT facilities must not be used to make, use, install, distribute, sell, hire, re-direct or otherwise process any copies of computer software, radio, TV, film or music for any purpose (either here or elsewhere) without licence

or without the permission of the copyright owner.

2. You must treat as confidential any information to which you gain access in using College ICT facilities and which is not on the face of it intended for unrestricted dissemination e.g. information posted in a virtual learning environment.

e) Security

The College operates and maintains a large and extensive networked computer system to support teaching and learning. These vital information processing and communication resources must be adequately protected so that the integrity and availability of these systems can be assured and the privacy of individual users protected.

1. Attempting to circumvent, remove or thwart College ICT security controls is not permitted.
2. Interfering with, or modification or alteration of software, computer configurations, settings, equipment, data files or websites without the written authorisation of a line manager or Director of Operations is not permitted.
3. Causing damage to College ICT facilities, or moving or removing such facilities without authorisation is not permitted.
4. Downloading, creating or using any program, tool or item of software designed to monitor damage, disrupt or interfere with the functioning of ICT facilities, user accounts or data is not permitted.

f) Disruption and mischief

Information systems provide a platform from which communication to your immediate circle of friends, professional peers, or global community is easily achievable. With this power comes responsibility.

1. Acting in a way which directly or indirectly causes disruption to others' use of College ICT facilities, or using College ICT facilities to disrupt the use of ICT facilities elsewhere is not permitted.
2. Using College ICT facilities to defame, harass, offend or hinder another person, by creation, transmission, storage, download or display of materials, or by any other means is not permitted.

g) Electronic messaging

Impersonating another person using email, online chat, web or other services is an offence under the terms of Computer Misuse Act 1990.

1. Sending anonymous emails or electronic messages or messages that do not correctly identify you as the sender, or messages which appear to originate from another person is not permitted.
2. Intentional transmission of unsolicited or unauthorised commercial or advertising material within the College or to other individuals or organisations is not permitted. Such material includes unsolicited email (spam), chain letters, hoax virus warnings, pyramid letters or other junk

mail of any kind.

h) Social media

The College has provided separate guidelines on use of social media by staff and students in relation to the College.

Possible consequences of unacceptable use

Violations of this Acceptable Use Policy may be investigated under the College's Conduct and Discipline of Students Procedure. The following actions may be taken by the College in response to a breach of this Policy:

- withdrawal of College ICT facilities;
- blocking or limiting network account access;
- disconnection and seizure of equipment that is in violation of this Policy;
- initiation of relevant disciplinary procedure for staff or student.

Where there is evidence of a criminal offence, the matter will be reported to the Police. The College will co-operate with the investigating authorities and disclose copies of any relevant data stored, appropriate logs and any hardware used (relevant to the investigation) to the Police in line with current legislation.

The Director of Operations may temporarily suspend the authority of any user of any system where there are reasonable grounds to suspect that a user has breached this Policy, pending an investigation.

Document control box			
Title	**Information Communications Technology Acceptable Usage Policy**		
Date approved	Jan 2016	Implementation date	Jan 2016
Next review date			
Version	1	Supersedes version	N/A
Approving body		Governors	
Quality Code consulted			
Member of staff responsible		Director of Operations	