Spurgeon's College Information Communications Technology Guidelines for Staff and Volunteers

1. Introduction

1. All staff and volunteers are expected to adhere to the College's ICT acceptable usage policy and guidelines for social media usage.

2. The College expects all of its electronic and computer facilities to be used in an effective and professional manner and encourages all staff and volunteers to develop the skills necessary to do so. These facilities are provided by the College at its own expense for its own business purposes to assist its staff and volunteers in carrying out their duties effectively. It is the responsibility of each member of staff and volunteer to ensure that this technology is used for proper business purposes and in a manner that does not compromise the College or its staff or volunteers in any way.

3. Staff and volunteers may sometimes need to use College equipment and access the College network while working remotely (e.g. via VPN), whether from home or while travelling. The standards set out in the College's ICT policies and guidelines apply whether or not College equipment and resources are being used.

4. Misuse of the internet or email can expose both you and the College to legal or financial liability. For example, you may enter into unintended contracts, breach copyright or licensing arrangements, incur liability for defamation or harassment or introduce viruses into the system. College ICT guidelines and polices are designed to safeguard both you and the College from such liabilities. It is important that you read all College policies on the use of ICT carefully and ensure that any use of the internet, social media or email is in accordance with its terms.

5. The Director of Operations is responsible for the monitoring and implementation of ICT policy and guidelines. If you have any questions you should contact the Director of Operations.

2. Confidentiality

1. Staff and volunteers should double check the recipient before pressing the send button on an email – not only can it be embarrassing if a message is sent to the wrong person, it can also result in the unintentional disclosure of confidential information about the College.

2. Where sensitive and confidential information needs to be sent via email for practical reasons, please be aware that email is essentially a non-confidential means of communication. Emails can easily be forwarded or archived without the original sender's knowledge. They may be read by persons other than those they are intended for.

3. Staff and volunteers should never assume that internal or external messages are necessarily private and confidential, even if marked as such. The internet is not a secure means of communication and third parties may be able to access or alter messages that have been sent or received. Do not send any information in an email which you would not be happy being publicly available. Matters of a sensitive or personal nature should not be transmitted by email unless absolutely unavoidable and if so, should be clearly marked in the message header as highly confidential. The confidentiality of internal communications can only be guaranteed if they are delivered personally by hand.

4. Internet communications should be treated as non-confidential. Anything sent through the Internet passes through a number of different computer systems, all with different levels of security. The confidentiality of messages may be compromised at any point along the way unless the messages are encrypted.

5. Staff and volunteers must not leave IT facilities signed in and unattended and potentially usable by some other person. Staff and volunteers are advised to 'lock' their computers when away from them to avoid potential breaches of confidentiality.

3. Email messages

1. Staff and volunteers should not transmit anything in an email that they would not be comfortable writing (or someone else reading) in a letter or a memorandum. Emails leave a retrievable record. Even when you think you have deleted information, it can remain on both your computer and on the College's back up system. Emails can be recovered as evidence in court proceedings and/or reviewed by regulators. Electronic messages are admissible as evidence in legal proceedings and have been used successfully in libel and discrimination cases.

2. Staff and volunteers must exercise due care when writing emails to avoid being rude or unnecessarily terse. Emails sent from Spurgeon's College may be interpreted by others as official statements. Users are responsible for ensuring that their content and tone is appropriate. Emails often need to be as formal and business-like as other forms of written correspondence.

3. If staff or volunteers receive an email containing material that is offensive or inappropriate to the office environment then they must delete it immediately. Such mail or fax must not be forwarded either internally or externally. The forwarding of messages such as jokes is not expressly forbidden, but staff and volunteers may not forward offensive material and should be careful about creating congestion on the system with frivolous messages, particularly those with large attachments.

4. You must not send (inside or outside work) any message in the College's name unless it is for a work-related purpose.

4. Passwords

1. Staff and volunteers must not allow other staff and volunteers to use their password, except with the express permission of the Director of Operations, their deputy or the Principal. If it is anticipated that someone may need access to the confidential files of staff and volunteers in their absence, they should arrange for the files to be copied to somewhere where that person can access them or give them access to the relevant personal folders.

5. Viruses

1. When using the College email system, be vigilant. Computer viruses are often sent by email and can cause significant damage to the College's information systems.

2. Any files or software downloaded from the Internet or brought from home must be virus checked before use. Staff and volunteers should not rely on their own PC to check for a virus any such programmes but should refer directly to the Directory of Operations. If you suspect that a file may contain a virus, do not open it and contact the Director of Operations immediately.

6. The Internet

1. Access to the internet during working time should be limited to matters relating to employment. However, you may make reasonable personal use of the internet provided it does not interfere with your duties and provided that use is strictly in accordance with the College's ICT acceptable usage policy.

2. Under no circumstances should information of a confidential or sensitive nature be placed on the Internet.

3. Information posted or viewed on the internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the Internet may be done only by express permission from the copyright holder. Staff and volunteers must not act in such a way as to breach copyright or the licensing conditions of any Internet site or computer programme.

4. Staff and volunteers must not commit the College to any form of contract through the Internet without the agreement of the Director of Operations.

5. Subscriptions to news groups, mailing lists and social networking websites are permitted when the subscription is for a work-related purpose. Any other such subscriptions are only permitted where their use does not interfere with the performance of duties by staff and volunteers or cause congestion on the system.

7. Interception of communications

1. The College does not as a matter of policy routinely monitor the use of the internet or the content of email messages sent or received by staff or volunteers. However, the College has a right to protect the security of its systems, check that use of the system is legitimate, investigate suspected wrongful acts and otherwise comply with legal obligations imposed upon it. To achieve these objectives, the College may carry out random spot checks on the system which may include accessing individual email messages or checking on specific Internet sites you have accessed.

2. The College also reserves the right to read the emails of staff and volunteers to check for business emails whilst they are absent or out of the office. The College may also access the voicemail of staff and volunteers to check for business calls whilst they are absent or out of the office. It may therefore be unavoidable that some personal messages will be read or heard.

8. Breaches of the College's ICT policies and guidelines

The College considers the use of ICT to be extremely important. If a member of staff or volunteer is found to be in breach of any of the College's ICT policies or guidelines then they will be disciplined in accordance with the Disciplinary Procedure and may be dismissed.

Document control box			
Title	**Information Communications Technology Guidelines for Staff and Volunteers**		
Date approved	January 2016	Implementation date	January 2016
Next review date			
Version	2	Supersedes version	1 (Feb 2013)
Approving body		Governors	
Quality Code consulted			
Member of staff responsible		Director of Operations	