

**STRATEGIC
GROUP POLICY SGP004****IT, INTERNET AND
EMAIL POLICY****LEADERSHIP****Written by:** Liam O'Loughlin**Date:** 07/02/2022**Revision:** 03**Doc Ref:** SGP004**Reviewed by:** Andrew Smith**VISION:****Our Vision:**

"To ensure that compliance with this policy is maintained and that all use of information technology software and equipment is conducted in line with the company's code of conduct".

We are realising our Vision by constantly reviewing and updating our Company Handbook to ensure the latest controls and guidance are in place.

COMMITMENT:

Arthur Civil Engineering Ltd provides access to vast information resources to help you do your job. The facilities to provide that access represent a considerable commitment of Company resources for telecommunications, networking, software, storage, etc. This policy is designed to help you understand our expectations for the use of those resources, and to help you use those resources wisely. We ask all our employees to take great care of our IT resources and to respect the letter of this Policy which, fundamentally, protects the Company as a whole.

We encourage the use of the internet and email for business purposes. All users must ensure that their use of these resources at all times protects the intellectual property of the Company, the confidentiality of information and the integrity of the IT environment. The Company reserves the right to make random checks on the use of the internet and email system to ensure that Company policy is being followed.

RESPONSIBILITY:**The Directors of Arthur Civil Engineering will:**

- Monitor compliance with this Privacy Notice Policy.
- Ensure Arthur Civil Engineering Ltd works with clients and their Privacy Notice Policies.
- Communicate this Policy to their employees to ensure awareness throughout the Company.

- Ensure sufficient provision of resources is made in order to implement the requirements of this Policy.

All Employees of Arthur Civil Engineering must ensure they:

Read and understand this Policy.

APPROACH:**INFORMATION TECHNOLOGY (I.T.)****Email**

- Email messages are Company property and for all purposes should be viewed in exactly the same way as hard copy communications. As with hard copy communications, all employees are expected to use email as an effective means of communicating business related issues.
- Email messages are to be used for Company-sanctioned activities in a manner that furthers the interests of the Company. Such communication must be consistent with other Company policies and have due regard for confidentiality, being both legal and ethical.
- Personal use of email in special circumstances or in an emergency is acceptable but all personal usage should be kept to a minimum. Such usage should respect the Company's values and be professional in its content at all times. Frivolous, derogatory or offending emails will not be tolerated and will be a matter for the Company's disciplinary procedure. Under no circumstances should email be used for sending or soliciting messages that harass, are obscene or promote a religious, political or other personal agenda not associated with a Company business function. Chain letters must not be commenced or forwarded under any circumstances.
- Please be aware that as inbound emails are checked for content, viruses and malware. We cannot guarantee that any personal emails will be received.
- Attachments received from external sources will normally be subject to virus scanning at the point of receipt into the Company networks prior to their usage or onward transmission. However, malicious content can slip through on occasions and we ask all employees to be particularly vigilant and report any suspicious content directly to the IT and Data Manager. If you suspect an attachment may be malicious, do not open it.
- Each employee email address is set up with an associated 'quarantine' (which aims to filter out unrecognised and potentially 'spam' email content). It is the responsibility of each employee to maintain and monitor their own quarantine to ensure that unwanted or malicious emails are blocked and to ensure the significant or important emails are not lost. If you suspect you are not receiving notifications of blocked emails please contact the IT and Data Manager.
- During your induction into the Company any relevant/applicable IT housekeeping rules will be fully explained to you and you will be required to comply with them at all times.

Email Signatures

- At Arthur Civil Engineering it is our policy that every email sent, including second responses, should contain an email signature. The signature is a standard template that every employee must display. When a new employee starts they will be issued with the standard email signature.
- Email signatures should **not** contain your job title or position and neither should they contain any qualifications you have obtained during your career. The Company displays an organogram in the office and on its website; at Arthur Civil Engineering we are all one team.

INTERNET

Internet Usage:

- Internet access and email facilities are provided for business use. Employees will be permitted to use these facilities for personal use for a *reasonable* amount of time provided that such use does not interfere with work or business operations. We expect all our employees to exercise their discernment and discretion when browsing the internet. Please be aware that access to certain websites may be restricted according to Company policy.
- Unnecessary or unauthorised internet usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies, and ties up printers and other shared resources. Unlawful internet usage may also produce negative publicity for the Company and expose the firm to significant legal liabilities.
- While our direct connection to the internet offers many benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. Whilst the IT and Data Manager holds primary responsibility for overseeing IT the overriding principle is that security is to be everyone's first concern and responsibility.

Inappropriate Usage:

- The display of any kind of sexually explicit image or document on any Company system is a breach of our policy on sexual harassment. In addition, sexually explicit material may not be stored, distributed, edited or recorded using our network or computing resources. If you find yourself connected accidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.
- Arthur Civil Engineering Ltd internet facilities and computing resources must not be used knowingly to violate the laws and regulations of the United Kingdom in any material way. Use of any Company resources for illegal activity is grounds for immediate dismissal, and we will cooperate with any legitimate law enforcement activity.
- Arthur Civil Engineering Ltd do not condone bullying in any form and our internet facilities and computing resources must not be used knowingly to undertake any form of bullying in particular any trolling on online forums.

- Arthur Civil Engineering Ltd internet facilities and computing resources must not be used knowingly to undertake gambling in any form.
- Use of Company internet access facilities to commit infractions such as misuse of Company assets or resources, sexual harassment, and misappropriation or theft of intellectual property are also prohibited and will be treated as 'gross misconduct' within the frame of our Disciplinary Policy.
- Please note: the content of this Clause "Inappropriate Usage" applies irrespective of the device that you use to access the internet and therefore includes mobile phones and tablets.

Monitoring & Inspection:

- We reserve the right at any time to install and use software in order to monitor and record all internet usage. We want you to be aware that our security systems are capable of recording each worldwide website visit, chat, newsgroup or email message, and file transfer into and out of our internal networks. We reserve the right to monitor such activity for our individual users and you are reminded that inappropriate use of our systems and software may constitute grounds for disciplinary action. We reserve the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.

Social Networks

- Irrespective of where or when employees use social networking sites (either during lunch breaks in the office, or at any time whilst at home or elsewhere) the requirements of this Clause "Social Networks" apply and do not contravene your entitlements under the Human Rights Act.
- We expect our employees to consider the impact their language and behaviour may have when discussing *any* subject on Facebook, Twitter, or equivalent sites. If it is brought to our attention that anyone has spoken or acted online in a way that is incompatible with our corporate values and potentially harmful to our corporate reputation, then disciplinary action may be taken and this may result in termination of employment/engagement.
- You are reminded that Company information, client data, and trade secrets may **never** be discussed on social networks. You may not discuss colleagues online in any capacity, save where they are party to a discussion and have implicitly granted you permission to do so. Any employee who breaches this requirement will be subject to disciplinary action and this may result in instant dismissal.

ELECTRONIC EQUIPMENT

Company Electronic Equipment

- Computer electronic equipment - including but not limited to laptops and smart devices - is an extremely important resource and must always be treated carefully and with respect. Employees should ensure that all computer equipment is kept clean and tidy at all times and hazards (such as food and drink) are kept well away from the equipment. We ask all

employees to treat Company equipment with care. Please refer to your individual Contract of Employment with regard to your liability in respect of Company equipment.

- All electrical equipment that constitutes part of an employee's workstation must be switched off (powered down) overnight, at weekends and when on holiday, this includes desktop PC's. Exceptions are allowed if remote access will be required before the employee next returns to the office.
- Company owned electronic equipment must be returned to the IT and Data Manager in the event of termination of employment, or at any time upon request.

Personal Electronic Equipment

- The Company discourages the use of personal electronic equipment to access Arthur Civil Engineering Ltd 's network and resources. The reason for this is linked to our strict security protocol. Therefore, if for any reason you need or desire to use your personal electronic equipment to access Arthur Civil Engineering Ltd 's network and resources you must ensure that personal electronic equipment is fully password enabled and that you take measures to update your passwords as necessary.
- You may not store any Company documentation on personal electronic equipment.
- Please also refer to the Company Handbook for information on the Company's limit of liability in regard of your personal property (which includes electronic equipment). Your personal electronic equipment is not covered under Arthur Civil Engineering Ltd 's support agreements and insurance arrangements.

General Security Protocols for Electronic Equipment

- Use PIN codes and/or fingerprint scanning to activate mobile phones.
- Voicemail must also be protected by a PIN code and/or fingerprint scanning to access.
- If device encryption is available please activate it.
- Any security device/application installed on Company devices must not be deactivated.
- Only approved security applications must be installed. Do not download free anti-virus products.
- Security updates must be enabled.
- Public wireless networks may not be secure; do not access unless you have optimised your own security protocols.
- Do not lend your device to any other party.
- Report any loss or theft of a device immediately to the IT and Data Manager; this is to ensure that the data is wiped remotely.

REMOVABLE MEDIA

- In line with our commitment to safeguard not only our own but our clients' and other third parties' confidential information, we require all employees to conform with our policy on removable media. For clarity, 'removable media' will include – amongst other things - CDs, DVDs, optical disks, external hard drives, USB memory sticks (pen drives or flash drives),

media card readers, Smart cards, SIM cards, and digital cameras. Misuse of removable media can result in:

- i. Disclosure of protected and restricted information as a consequence of loss or theft;
 - ii. Contamination of Company networks or equipment through the introduction of viruses
 - iii. Through the transfer of data from one form of IT equipment to another;
 - iv. Potential legal action against the Company or individuals as a result of information loss or misuse;
 - v. Significant reputational damage for Arthur Civil Engineering Ltd.
- The only equipment and media that should be used to connect to Company equipment or the network is equipment and media that has been purchased by the Company and approved by the Directors.
 - Data stored on removal media must be backed up/copied on the source system or a networked computer.
 - All removable media devices must be encrypted/secured in line with the provisions of this IT, Internet & Email Policy.
 - Any suspected breaches of information security (loss/damage/theft) must be immediately reported to the IT and Data Manager.
 - No third party may receive data or extract information from the Company's network, information stores or IT equipment without the explicit agreement of the IT and Data Manager. Furthermore, the third party will be required to sign a Non-Disclosure and Confidentiality Agreement and must be made fully aware of our Data Protection Policy.
 - Damaged or obsolete removal media must be securely disposed of to avoid data leakage. Its content must be erased, and this will be done by the IT and Data Manager.

LICENSING AND COPYRIGHT

- Any software or files downloaded via the internet into the Company network become the property of the Company. Any such files or software may be used only in ways that are consistent with their licences or copyrights. No employee may use Company facilities to knowingly download or distribute pirated software or data.
- If you need to download software you are required to exercise due care, consideration and judgement to ensure that in so doing you do not compromise the Company in any way. If in any doubt whatsoever, please speak to the IT and Data Manager in the first instance.

EMAIL SIGNATURE FORMAT (NOT TO BE CHANGED):

Regards,

Joe

Joe Bloggs



Mob: [Insert Mobile Number](#) | Tel: [+44 \(0\)1509 648099](#) | Email: [Insert Email Address](#) |
 Web: www.arthurcivilengineering.com

Unit 1 Beaumont Court, Prince William Road, Loughborough, LE11 5DA



This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error, please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

REVISION STATUS:

Rev.	Date	Description if Addition (A), Deletion (D) or Substitution (S)	Approved by:	
1.1	01	05.07.2018	Written by Liam O'Loughlin	Andrew Smith
1.2	02	15.08.2018	Email Signatures (Liam O'Loughlin)	Andrew Smith
1.3	03	07.02.2022	2022 Review	Andrew Smith

The information contained in this Policy applies to all employees of Arthur Civil Engineering Limited ('Arthur Civil Engineering Ltd' or 'the Company') subject to any qualifying conditions described. This policy should be read in conjunction with your Contract of Employment and the Company Handbook. The Company may amend and extend the contents of this document at any time, subject to statutory and/or operational requirements. If you require any clarification in respect of this Policy, please speak in the first instance to one of the Directors.