Information Technology Policy

The overall purpose of the IMPRESS information technology system is to ensure that communication to, from and within IMPRESS is efficient and quick, that information-sharing is timely and appropriately comprehensive, and that IMPRESS can make optimal use of the benefits of electronic technology in pursuit of its goals.

Communication & access to information

Each IMPRESS staff member is allocated a computer and an e-mail address upon joining IMPRESS.

Files on the IMPRESS Server are for use only by members of IMPRESS staff, Board and committees (representatives) and each representative is given personal access to these files.

Representatives should ensure the integrity of their password and not divulge this. If a representative suspects that password security has been compromised, he/she should alert the Company Secretary. All electronic devices (eg laptops, iPhones, iPads) accessing IMPRESS data must be protected by a secure password.

Allocation of computers, email addresses, passwords etc. is done by the Company Secretary, to whom any queries should be directed. On your first day at IMPRESS, you should be given essential login details. An induction session on IT systems with the Company Secretary will be arranged for you, normally on your first day of employment.

Members of staff should use the IMPRESS server to store all their work files. IMPRESS work files must not be stored on the local hard drive of a staff member's computer (typically drives C and D). Work stored on these drives is not accessible to other staff, is NOT backed up and is lost if the hard disk fails. Failure to store all work files on the IMPRESS service could result in a data breach according to the General Data Protection Regulation (GDPR).

The Company Secretary aims to provide high-quality, responsive user support which meets the needs of staff. To help him achieve this, he needs prior notification of non-emergency tasks such as relocation of equipment, setting up accounts for new staff, requests for laptops and requests for software installation. This will enable the Company Secretary to schedule time for these tasks and be able to respond to urgent requests for help. If you fail to give adequate notice, we may not be able to meet your deadline or supply you with the equipment you require.

If a staff member leaves his/her computer for a period of time he/she should save all open documents and lock it or log out.

If a staff member encounters a problem with the computer, he/she should first attempt to resolve it by checking cables and/or by restarting the machine. If this does not solve the problem, notify the Company Secretary who will try to resolve the issue. If the Company Secretary is unable to resolve the problem, it will be raised to IT support company Natpoint (020 8951 0050).

Internet and Email

IMPRESS encourages its employees to use email and the internet at work where this can save time and expense. However, it requires that employees follow the rules below. It is a term of each employee's contract that he/she complies with these rules, and any serious breach could lead to dismissal. Any employee who is unsure about whether or not something he/she proposes to do might breach this email and internet policy should seek advice from the Company Secretary. If an employee is concerned that their actions may have resulted in a data breach under GDPR they must follow the IMPRESS data breach protocol.

Although IMPRESS encourages the use of email and the internet where appropriate, their use entails some risks. For example, employees must take care not to introduce viruses to the system and must take proper account of the security advice below. Employees must also ensure that they do not send untrue statements about others in emails as IMPRESS could face legal action for libel and be liable for damages.

These rules are designed to minimise the legal risks to the organisation when its employees use email at work and access the internet. Where something is not specifically covered in this policy, employees should seek advice from the Company Secretary.

Technology and the law change regularly and this policy will be updated to account for changes as and when necessary. Employees will be informed when the policy has changed but it is their responsibility to read the latest version of this document.

<u>Use of email</u>

Contents of emails

Emails that employees intend to send should be checked carefully. Email should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter is equally unacceptable in an email. Staff should write with the awareness that any email they send could end up in the public domain.

The use of email to send or forward messages that are defamatory, obscene or otherwise inappropriate will be treated as misconduct under the appropriate disciplinary procedure. In serious cases this could be regarded as gross misconduct and lead to summary dismissal.

Equally, if an employee receives an obscene or defamatory email, whether unwittingly or otherwise and from whatever source, he/she should not forward it to any other address.

CCing

Employees should exercise care not to copy emails automatically to all those copied in to the original message to which they are replying. Doing so may result in disclosure

of confidential information to the wrong person and result in a data breach and a breach of IMPRESS' obligations under GDPR.

Attachments

Employees should not attach any files that may contain a virus to emails, as the organisation could be liable to the recipient for loss suffered. IMPRESS has virus-checking in place but, if in doubt, employees should check with the Company Secretary.

Employees should exercise care when receiving emails with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

Personal use of email

Although the email system is primarily for business use, the organisation understands that employees may on occasion need to send or receive personal emails using their work address.

When sending personal emails, employees should show the same care as when sending work emails.

Monitoring of email

IMPRESS reserves the right to monitor employees' emails, but will endeavour to inform an affected employee when this is to happen and the reasons for it. IMPRESS considers the following to be valid reasons for checking an employee's email:

- If the employee is absent for any reason and communications must be checked for the smooth running of the business to continue.
- If the organisation suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity (although the organisation understands that it is possible for employees inadvertently to receive such material and they will have the opportunity to explain if this is the case).
- If the organisation suspects that an employee has been using the email system to send and receive an excessive number of personal communications.
- If the organisation suspects that the employee is sending or receiving emails that are detrimental to the organisation.

When monitoring emails, IMPRESS will, save in exceptional circumstances, confine itself to looking at the address and heading of the emails. Employees should mark any personal emails as such and encourage those who send them to do the same. The organisation will avoid, where possible, opening emails clearly marked as private or personal.

The organisation reserves the right to retain information that it has gathered on employees' use of email for a period of one year

Use of internet

Authorised internet users

Where an employee has been provided with a computer with internet access at his/her desk, he/she may use the internet at work.

Sensible internet use

IMPRESS encourages employees to become familiar with the internet and does not currently impose any time limitation on work-related internet use. IMPRESS trusts employees not to abuse the latitude given to them, but if this trust is abused it reserves the right to alter the policy in this respect.

Removing internet access

IMPRESS reserves the right to deny internet access to any employee at work, although in such a case it will endeavour to give reasons for doing so.

Registering on websites

Many sites that could be useful for the organisation require registration.

Employees wishing to register as a user of a website for work purposes are encouraged to do so.

Licences and contracts

Some websites require IMPRESS to enter into licence or contract terms. The terms should be printed off and sent for approval in advance or emailed to the Company Secretary before an employee agrees to them on the organisation's behalf. In most cases, there will be no objection to the terms. Employees should, however, always consider whether or not the information is from a reputable source and is likely to be accurate and kept up to date, as most such contract terms will exclude liability for accuracy of free information.

Downloading files and software

Employees should download files on to only those PCs with virus checking software and should check how long the download will take. If there is any uncertainty as to whether or not the software is virus-free or whether the time the download will take is reasonable, the Company Secretary should be consulted.

Using other software and hardware at work

Employees are not allowed to bring software or hardware into the office without the Company Secretary's consent.

Personal use of the internet

Although the email system is primarily for business use, IMPRESS understands that employees may on occasion need to use the internet for personal purposes. Employees may access the internet at work for personal purposes provided that:

- the internet is not used to access offensive or illegal material, such as material containing racist terminology or nudity;
- they do not enter into any contracts or commitments in the name of or on behalf of the organisation; and

- they do not order goods in the organisation's name.

Monitoring of internet access at work

IMPRESS reserves the right to monitor employees' internet usage, but will endeavour to inform an affected employee when this is to happen and the reasons for it. IMPRESS considers the following to be valid reasons for checking an employee's internet usage:

- If the organisation suspects that the employee has been viewing offensive or illegal material, such as material containing racist terminology or nudity (although the organisation understands that it is possible for employees inadvertently to view such material and they will have the opportunity to explain if this is the case).
- If the organisation suspects that the employee has been spending an excessive amount of time viewing websites that are not work related.

IMPRESS reserves the right to retain information that it has gathered on employees' use of the internet for a period of one year.

General

The aim of these rules is to be helpful, and to set guidelines on the use of email and the internet at work for the smooth and efficient running of the business.

If there is anything in these rules that an employee considers to be unworkable or does not understand, he/she should notify the Company Secretary.

Self-employed contractors, agency workers or any other individuals working temporarily in the organisation should be made aware of the rules regarding the use of email and the internet.

New members of staff should be shown this policy as part of their induction.

Storage on the IMPRESS Server

1. Security

Security Information

You have been granted access to the IMPRESS server. You must ensure that none of your security information is disclosed to anyone else because you and your employer will be responsible for all activities which occur when someone is logged in using your security information. It is your responsibility to immediately notify the Company Secretary of any unauthorised use of any of your security information or any other breach of security.

Disclosing your security information to another person may be considered a disciplinary offence.

Confidentiality

The materials provided on the IMPRESS server are potentially sensitive and may be of a confidential nature. You may only use or disclose materials to another person with the consent of the author or the owner of copyright in the material.

In particular, you must also take all reasonable care to prevent others from gaining unauthorised access. This includes not leaving your screen unattended while it is displaying confidential information and always logging out from this secure section when away from your computer.

The security of the system depends on the responsible behaviour of each user.

2. Code of conduct

You agree that you will not:

- use the IMPRESS server for any commercial purpose for purposes other than IMPRESS-related work;
- store anything on the IMPRESS server which is unlawful, abusive, obscene, offensive, defamatory or which threatens to bring IMPRESS into disrepute;
- store any content on the IMPRESS server that promotes any illegal activity;
- disrupt the intended use of the IMPRESS server;
- compromise the privacy of users;
- store any content on the IMPRESS server which you do not have the right to post or use or which infringes any third party's rights;
- store on the IMPRESS server any material containing viruses or files which may cause damage to computer software or hardware or that affect the performance of the server;
- impersonate or misrepresent any other person or entity while using the IMPRESS server;
- attempt to gain unauthorised access to any part of the IMPRESS server; or
- violate any applicable local, national or international law or regulation while using the IMPRESS server.

You agree that you will comply with all data protection and information security policies.

IMPRESS will be entitled at its discretion to remove anything which is transmitted to, from or via the IMPRESS server or stored on the server which, in its opinion, is objectionable or in any way does not comply with the terms and conditions of use of the server. IMPRESS will not accept any liability for doing this.

IMPRESS cannot be responsible for any damage caused by a misuse of your data.

3. Legal Information: Privacy Policy

IMPRESS takes individuals' right to privacy very seriously and is registered under the Data Protection Act 1998 as a Data Controller. Should you wish to see or amend any of the information that IMPRESS holds about you and your use of the IMPRESS server, please contact the Company Secretary.

You may only store personal information about a third party (such as a name, address, e-mail address or photo) on the IMPRESS server, where this storage and processing complies with our data protection policies, that is, conforms with the purposes of IMRPESS related activity in the privacy statement and where you have the consent of that individual obtained through our consent declaration protocols. You must never post identifying details that may prejudice the rights, freedoms or legitimate interests of that person. Sensitive data relating to such things as a named person's health, sexuality or trade union membership should only be stored on the IMPRESS server with the express consent of that individual and that consent is obtained through our consent declaration protocols. Should you have any concerns arising from the use of personal data/information, please contact the Company Secretary. Contravention of data protection legislation may be a criminal offence.

Data Subject Access, Objection, Rectification and Erasure Requests

Under GDPR individuals can find out if we hold any personal information by making a 'data subject access request'; object to our storage or processing of their information or seek inaccurate information rectified or any data erased. You need to inform the Company Secretary as soon as possible if someone emails, phones or writes to us making one of the following requests:

- "Data Subject Access Request"
- "Data Subject Rectification Request"
- "Data Subject Erasure Request"
- "Data Use Objection"

If you are unsure as to whether an individual is making one of the following requests, you should seek clarification from them as soon as practicable. The Company Secretary will then do a preliminary assessment to determine whether to grant the request. Where an access request is granted, we will provide a Data Subject Request Notification. Where we do not grant a request, we will write to the data subject, providing reasons for why we are not granting the request and informing them of their right to complain to the Information Commissioner's Office.

Data Breach Protocol

The GDPR describes a data breach as:

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

What you need to do if you think there has been a data breach:

1. Let the Company Secretary know, as soon as you are aware of any potential breach
2. Log the data breach in the request database (over the phone or in writing) *
3. The Company Secretary will then do a preliminary assessment to determine if they consider the breach is likely to pose a risk to the rights and freedoms of any person

4. If necessary, the Company Secretary will inform the ICO and any affected party of the breach, and take any further steps

To log a data breach, we will need the following information:

(a) a description of the data breach including, where possible, the categories of data, the number of affected parties concerned, and the number of records concerned;
(b) the likely consequences of the data breach;
(c) the measures IMPRESS has taken or intend to take to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Data Security

We have a number of security measures in place to ensure the data we store and process are secure including:

- Storing data in our password-protected CRM, which is hosted on very secure Microsoft London servers;
- Retaining ongoing support from industry-leading IT companies for both our CRM and our office servers, ensuring that our data security is always monitored and up to date;
- Keeping two forms of backup: a backup in the office, and a Disaster Recovery backup that takes a backup of the main and exchange server every hour and automatically sends these to a data centre that is owned and operated by our external IT company;
- Encrypting our server and backups of our server. The server is protected by hardware firewall and an advanced comprehensive gateway security suite;
- Only allowing staff to access the server when in the office, or through a 2-factor authentication VPN connection when outside the office;
- Utilising a secure digital board portal solution for sharing of confidential board data rather than distributing it by email, post or other channels.

IMPRESS does not warrant that the functions and materials contained on its server will always be uninterrupted or error free, or that any defects will be corrected, or that the server are free of viruses or bugs, or that the materials contained in the site represent the full functionality, accuracy and reliability of the materials.

We invite you to bring to IMPRESS's attention any material you believe to be factually inaccurate. Please notify us by forwarding a copy of the material and your comments by email to the Company Secretary.

Approved by the Board	14/11/2017	Last updated	15/05/2018