Information Technology and Communications Policy

1. Purpose

1.1. 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.

1.2. Impress reserves the right to access and monitor the use of all Company-owned digital devices, including monitoring Internet, telephone and email use. Impress also monitors access to its networks via private devices.

1.3. Nothing in this policy prevents Impress' storage and processing of data for the purposes of discharging its regulatory duties, in accordance with Impress' privacy policy.

1.4. 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.

1.5. If there is anything in these rules that an employee considers to be unworkable or does not understand, they should notify Impress Secretary.

1.6. 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.

2. Communication & Access to Information

2.1. Each Impress staff member is allocated a computer and an e-mail address upon joining Impress. You must take the appropriate steps to guard against unauthorised access to, alteration, accidental loss, disclosure or destruction of data.

2.2. 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.

2.3. Representatives should ensure the integrity of their passwords and not divulge this. If a representative suspects that password security has been compromised, they should alert Impress Secretary. All electronic devices (e.g. laptops, mobile phones, mobile devices such as tablets) accessing Impress data must be protected by a secure password.

2.4. Allocation of computers, email addresses, passwords, etc. is done by Impress Secretary, to whom any queries should be directed. On your first day at Impress, you should be given essential login details and an induction session on IT systems with Impress Secretary will be arranged for you.

2.5. 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).

2.6. Impress Secretary aims to provide high-quality, responsive user support, which meets the needs of staff. To help them achieve this, they need 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 Impress Secretary to schedule time for these tasks and be able to respond to urgent requests for help. If you fail to give adequate notice, then we may not be able to meet your deadline or supply you with the equipment you require.

2.7. If a staff member leaves their computer for a period of time, then they should save all open documents and lock it or log out.

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

3. Internet and Email

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

3.2. 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.

3.3. 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 Impress Secretary.

3.4. 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.

3.5. Use of email

- *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, they should not forward it to any other address.

- *CC-ing*
    - Employees should exercise care not to copy emails automatically to all those copied into the original message to which they are replying. Doing so may result in the 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 the loss suffered. Impress has virus-checking in place but, if in doubt, employees should check with Impress 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 Internet use and email*

  - Impress reserves the right to monitor employees' Internet use and 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 Internet use and 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 Internet use and emails, Impress will, save in exceptional circumstances, confine itself to looking at the domain and address and heading of emails. Employees should mark any personal emails as such and encourage those who send them to do the same.
  - The organisation reserves the right to retain information that it has gathered on employees' use of email for a period of 18 months.

- *Use of Internet*

  - *Authorised Internet* users: Where an employee has been provided with a computer with Internet access at their desk, they 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 emailed to Impress 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, Impress Secretary should be consulted.
    - *Using other software and hardware at work*: Employees are not allowed to bring software or hardware into the office without Impress Secretary's consent.

4. Personal use of the Internet

4.1. 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.

5. Storage on the Impress Server

5.1. 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 that occur when someone is logged in using your security information. It is your responsibility to immediately notify Impress 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 offense.

- 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 the copyright in the material.
    - 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.
- 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 that 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.

- Legal Information: Privacy Policy

    - Impress takes individuals' right to privacy very seriously and is registered under the Data Protection Act 2018 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 Impress 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 Impress related activity in the privacy statement and where you have the consent of that individual obtained through our consent 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 protocols. Should you have any concerns arising from the use of personal data/information, please contact Impress Secretary. Contravention of data protection legislation may be a criminal offence.

6 Data Protection

6.1. Impress is fully committed to compliance with the requirements of the Data Protection Act 2018 and all other data protection legislation currently in action. The Regulation applies to anyone processing personal data and sets out principles, that should be followed and gives rights to those whose data is being processed.

6.2. To this end, Impress endorses fully and adheres to the Data Protection Principles listed below. When processing data we will ensure that it is:

- processed lawfully, fairly and in a transparent way ('lawfulness, fairness and transparency');
- processed no further than the legitimate purposes for which that data was collected ('purpose limitation');
- limited to what is necessary in relation to the purpose ('data minimisation');
- accurate and kept up to date ('accuracy');
- kept in a form that permits identification of the data subject for no longer than is necessary ('storage limitation');
- processed in a manner that ensures the security of that personal data ('integrity and confidentiality');
- processed by a controller who can demonstrate compliance with the principles ('accountability').

6.3. These rights must be observed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, Impress will:

- observe fully the conditions regarding having a lawful basis to process personal information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information only to the extent that it is necessary to fulfil operational needs or to comply with any legal requirements;
- ensure the information held is accurate and up to date;
- ensure that the information is held for no longer than is necessary;
- ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Act 2018 (i.e. the right to be informed that processing is being undertaken, to access personal information on request; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information);
- take appropriate technical and organisational security measures to safeguard personal information;

- ensure that personal information is not transferred outside the EU, to other countries or international organisations without an adequate level of protection.

7. Employees' Personal Information

7.1. Throughout employment and for as long as is necessary after the termination of employment, Impress will need to process data about you. The kind of data that Impress will process includes:

- any references obtained during recruitment;
- details of terms of employment;
- payroll details;
- tax and national insurance information;
- details of job duties;
- details of health and sickness absence records;
- details of holiday records;
- information about performance;
- details of any disciplinary and grievance investigations and proceedings;
- training records;
- contact names and addresses;
- correspondence with Impress and other information that you have given Impress.

7.2. Impress believes that those records used are consistent with the employment relationship between Impress and yourself within the data protection principles. The data Impress holds will be for management and administrative use only, but Impress may, from time to time, need to disclose some data it holds about you to relevant third parties, for example: where legally obliged to do so by HM Revenue & Customs, where requested to do so by yourself for the purpose of giving a reference or in relation to maintenance support and/or the hosting of data in relation to the provision of insurance.

7.3. In some cases, Impress may hold sensitive data, which is defined by the legislation as special categories of personal data, about you. For example, this could be information about health, racial or ethnic origin, criminal convictions, trade union membership or religious beliefs. This information may be processed not only to meet the Impress's legal responsibilities but, for example: for purposes of personnel management and administration, suitability for employment and to comply with equal opportunity legislation. Since this information is considered sensitive, the processing of it may cause concern or distress; you will be asked to give express consent for this information to be processed unless Impress has a specific legal requirement to process such data.

8. Access to Data

8.1. You may, within a period of 1 month of a written request, inspect and/or have a copy, subject to the requirements of the legislation, of information in your own personnel file and/or other specified personal data and, if necessary, require corrections should such records be faulty. If you wish to do so, then you must make

a written request to your Line Manager. Impress is entitled to change the above provisions at any time at its discretion.

8.2. Under GDPR individuals can find out if we hold any personal information by making a 'data subject access request'. Please refer to section 9 of our Privacy Notice for information on how to deal with such request.

8.3. 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:
  - Let the Impress Secretary know, as soon as you are aware of any potential breach;
  - Log the data breach in the request database (over the phone or in writing)*;
  - The Impress 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;
  - If necessary, the Impress 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 description of the data breach including, where possible, the categories of data, the number of affected parties concerned, and the number of records concerned;
  - The likely consequences of the data breach;
  - The measures Impress has taken or intends to take to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- Data Security
  - Employer's responsibilities:
    - 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 a hardware firewall and an advanced comprehensive gateway security suite;
        - 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 is free of viruses or bugs, or that the materials contained in the site represent the full functionality, accuracy and reliability of the materials.
    - Employees responsibilities:
        - You are responsible for ensuring that any personal data that you hold and process as part of your job role is stored securely.
        - You must ensure that personal information is not disclosed orally, in writing, via web pages, or by any other means, accidentally or otherwise, to any unauthorised third party. You should note that unauthorised disclosure may result in action under the Disciplinary Procedure, which may include dismissal for gross misconduct.
        - Personal information kept in physical copy should be kept in a locked filing cabinet, drawer, or safe. Electronic data should be coded, encrypted, or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.
        - When travelling with a device containing personal data, you must ensure both the device and data is password protected. The device should be kept secure and, where possible, it should be locked away out of sight, for example in the boot of a car. You should avoid travelling with hard copies of personal data where there is secure electronic storage available. When it is essential to travel with hard copies of personal data this should be kept securely in a bag and where possible locked away out of sight, for example in the boot of a car.
    - Notifying breaches:
        - A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.
        - The following are examples of data breaches:
            - access by an unauthorised third party;
            - deliberate or accidental action (or inaction) by a data controller or data processor;
            - sending personal data to an incorrect recipient;
            - computing devices containing personal data being lost or stolen;
            - alteration of personal data without permission;

        - loss of availability of personal data.
    - Investigation and notification:
        - In the event that we become aware of a breach, or a potential breach, an investigation will be carried out.
        - Impress will undertake to notify the Information Commissioner of a breach that is likely to pose a risk to people's rights and freedoms without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.
        - Impress will undertake to notify the individual whose data is the subject of a breach if there is a high risk to people's rights and freedoms without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.
    - Record of breaches: Impress records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under the Data Protection Act 2018. It records the facts relating to the breach, its effects and the remedial action taken.

We are committed to reviewing our policy and good practice annually.

Approved by: The Board of Impress

Date: 12 December 2023

Review Date: 12 December 2025