Staff Data Protection Protocol

1 Introduction

This protocol establishes guidelines covering how Impress the Examiner Ltd (the Company)'s data should be used and managed in order to provide a safe and confidential service to our clients, tutors and staff which complies with the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulations (UK GDPR) together referred to as the 'data protection legislation'.

The protocol applies to all staff (company employees, tutors, contractors) and anyone who directly or indirectly supports our services and uses the Company's data to do so.

2 Requirements of the data protection legislation (GDPR)

Under the data protection legislation the Company and its data processors (i.e. staff) are required by law to work with personal information responsibly, taking the individuals to whom the information refers into account. In addition, we are required to manage data breaches and data subject access requests (see below) in particular ways and within given timeframes.

All personal information should be worked with according to the Company's policies, procedures and protocols in order to protect the personal information of clients, client students and staff.

2.1 Data breaches

"A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data" (Information Commissioner's Office (ICO) website September 2021). Data breaches can include, amongst other things, an e-mail virus infecting personal information, a portable device with personal data on it being lost or stolen, or unauthorised personnel having access to the data.

In the event of a data breach the Company has **3 days (72 hours)** to assess the situation, decide whether it is necessary to inform the ICO and the individuals whose data has been affected, and address the issue.

Any data breach MUST be reported as soon as possible to the Data Protection Lead.

2.2 Data Subject Access Requests (SAR)

Clients, the students we tutor and all company staff can request to exercise the following rights with regard to any personal information of theirs that the Company works with:

a) the right of access,
b) the right to rectification,
c) the right to erasure,

d) the right to restrict processing,
e) the right to data portability,
f) the right to object,
g) rights in relation to automated decision making and profiling.

In some cases, for example where the information is part of a legal case or where complying with the request would impact another individual's rights, such requests might be refused. In most circumstances, however, the Company will be required to comply with the request.

A detailed response, whatever action is to be taken, must be supplied within **one calendar month** and so SAR's must be acted upon **as soon as possible**.

If you receive a written or verbal SAR, follow the Company's Data Subject Access Request Procedure below.

NOTE: Subject access requests can be verbal; according to the data protection legislation we cannot insist on a written request.

3 Working with personal information

3.1 General principles

- All personal information must be treated with respect and awareness.
- Use of company data for anything other than the purpose for which it was intended is strictly forbidden.
- Work with company data within the IT structures specified by the Company.
- Do not attempt to bypass security measures set up by the Company to secure its data or the data of its clients.
- Consider the physical security of high risk or sensitive information (see Annexure below for examples) and, for example, use locked filing cabinets or cupboards for storage of documents or electronic equipment used to work with personal data.
- Keep secured and do not leave valuables or items such as unencrypted USB drives, smart phones, tablets or laptops on display.
- Avoid duplication of information wherever possible.
- Desktop and portable device screens should, where possible, be angled away from doors and windows so that confidential information cannot be read by others.

3.2 Maintain data integrity

- Regularly check (at least once a year) that your data is up-to-date and that old data have been deleted. Refer to the Company's Data Retention Policy for guidance on how long to keep information, request a copy from your point of contact if required.
- Ensure that information you work with is easily retrievable. In the event of a SAR staff must retrieve all relevant requested information wherever it is held within the specified timeframe.

- Ensure that company information held remotely is securely transferred to the Company on completion of your contract or employment.

4 E-mail

E-mail is an inherently insecure medium open to malicious attacks of various kinds and to unintentional human error. The company therefore requires that staff:

- Do not send high risk or sensitive information by e-mail unless it is encrypted (see Annexure below for examples of high risk and sensitive information). Always check for safe delivery.
- Make sure your e-mail software does not default to the 'reply to all' button – only use 'reply all' when necessary and with awareness.
- Do not use e-mail to store high risk or sensitive information.
- If you send high risk personal data or sensitive information to a colleague, indicate in the e-mail subject line that the e-mail contains sensitive information so that the recipient can exercise caution about where and when they open it.
- Do not keep e-mails longer than necessary; go through your e-mails and delete those which are not needed at least once a year.
- File e-mails you choose to keep (e.g. in folders within our Inbox) so that you can easily find them if any individual you have corresponded with makes a data subject access request (SAR).

5 Working remotely/using mobile devices

5.1 Security

5.1.1 Malware Prevention

- Install professional anti-malware software on all equipment used to work with or access company data.
- Internet routers used to work from home should be passworded and include a robust firewall.

5.1.2 Passwords

- Keep passwords private. Do not share company passwords with anyone else unless authorised by the Company's Data Protection Lead in the event of an emergency.
- Upon termination of employment or contract (for whatever reason) the staff member concerned is required to provide details of any company passwords they use to access company accounts and data to the Company.

5.1.3 Encryption

When sensitive personal information is processed remotely (see Annexure below) it must be stored and transmitted in a professional standard encrypted form.

- Electronic keys for encryption, e.g. passwords, must be appropriately managed so that the Company can always access the information.

- Encryption keys, e.g. passwords, must not be communicated via the same channel as the encrypted data.
- When data is encrypted by the user, a procedure for the management of electronic encryption keys must be established to ensure information can be accessed by authorised users when needed.

5.2 Personal mobile device protocol

- Do not store company data on privately owned equipment or in e-mails.
- Control access to devices used. Use fingerprint scanning if available, otherwise by password or PIN if neither fingerprint nor password is possible.
- Use a screen or device lock that will trigger after a short period of inactivity (no longer than 10 minutes).
- Do not share devices used to work with personal information with others including members of your household.
- Configure your device to enable you to remote-wipe it should it be lost or stolen.
- When accessing your e-mail, exercise caution to ensure that you do not download unencrypted high risk personal data or sensitive information to an insecure device.
- Do not leave your device unattended in situations where others could access it and ensure it is physically secure at all times.
- The loss or theft of a mobile device that holds company data must be reported immediately in accordance with the Company's Data Breach Procedure.
- Do not process or view High Risk Data in public places.
- The company reserves the right to prevent access to company files or services by any device that is considered a risk.
- Do not use public WiFi spots if you are using a personally owned device to work with high risk data (see Annexure below). Disable Bluetooth and WiFi if they are not needed to help prevent hacking.
- If you are using a personally owned device to work with high risk data the data must be encrypted.
- Keep your device's software up to date. This includes operating systems, applications, and anti-virus and malware protections.
- On ceasing to work for the Company, ensure all company data is deleted securely from your device.
- Remove company data from the device before disposing of it, selling it or passing it onto another individual. Ideally, reset the device to factory defaults.
- In exceptional circumstances the Company may require that data on a personally owned device be remotely wiped (e.g. in the event of loss or theft of the device).

6 Consequences of non-compliance

A breach of this protocol by staff may lead to the termination of their contract or engagement. This will apply whether the breach occurs during or outside normal working hours and at whatever location.

Staff concerned in any incident are required to co-operate with any investigation into a suspected breach, which may include providing the Company with access to any devices concerned.

If a data incident takes place as a result of staff breaching of this protocol which has a significant negative impact on data subjects (the individual(s) whose data are concerned), litigation may result.

7 Contacts

If you have any queries or if you need to report a data breach or SAR contact:

Data breaches should be reported to:

Tamara Caldwell (Data Protection Lead)
E-mail: tcaldwell@impresstheexaminer.com
MOB: 03332 12 05 75

Data subject access requests (SARs) should be reported to:

Fatima Hajnal,
E-mail: admin@impresstheexaminer.com,
MOB: 03332 12 05 75

I have read the Impress the Examiner Ltd Staff Data Protection Protocol.

Signed: Dated:
[STAFF NAME]

Annexure

High risk, special category or sensitive information

The following are examples of high risk special category or sensitive information:

- Information relating to students' backgrounds, grades, personal situation and related or comparable information.
- Any data relating to identifiable individuals' health, disability, ethnicity, race, sex life, sexual orientation, trade union membership, political or religious affiliations, genetics or biometrics (where used for ID purposes, e.g. CCTV cameras).
- Any set of data relating to more than 50 living, identifiable individuals, including, but not limited to staff, students, clients.
- Any set of data relating to 10 or more living, identifiable individuals that could be used for fraud or identity theft, including but not limited to, bank account or credit card details, national insurance number, personal contact details, date of birth, salary.
- Information relating to 10 or more staff's performance, grading, promotion or personal and family lives.
- Although criminal offence data is dealt with under different legislation, for the purposes of data protection any data relating to identifiable individuals' commission or alleged commission of an offence.
- Information provided to the Company in confidence.
- Company finance data.
- Health records of any living, identifiable individual.
- Information that would attract legal professional privilege.