Data Security Policy

Our policy on data protection

As a postal operator, Foojit ("the Company") processes personal data in relation to its own staff, work-seekers, individual client contacts and mail recipients.

The Company abides by the principles of the Data Protection Act 1998 set out below.

Foojit holds data on individuals for the following general purposes:

- Staff administration
- Mail distribution
- Accounts and records
- Administration and processing of work-seekers' personal data for the purposes of work-finding services

The Data Protection Act 1998 requires Foojit as data controller to process data in accordance with the principles of data protection. These require that data shall be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subjects rights
- Kept securely
- Not transferred to countries outside the European Economic Area without adequate protection.

Personal data means data relating to a living individual who can be identified from the data or from the data together with other information, which is in the possession of, or is likely to come into possession of, Foojit.

Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on the data. It includes organising, adapting and amending the data, retrieval, consultation and use of the data, disclosing and erasure or destruction of the data. It is difficult to envisage any activity involving data which does not amount to processing. It applies to any processing that is carried out on computer, including any type of computer however described, such as main frame, desktop, laptop or palm top.

Data should be reviewed on a regular basis to ensure that it is accurate, relevant and up to date.

Data may only be processed with the consent of the person whose data is held. Therefore if they have not consented to their personal details being passed to a third party this may constitute a breach of the Data Protection Act 1998. As Foojit act as intermediaries in the postal process and have no control over personal mailing data, it is the stated responsibility of their clients to ensure this data is processed either by a) the individual's personal consent or b) via the Mailing Preference Service (MPS) to prevent unwanted use of personal data.

Data Security Policy

By instructing Foojit to look for work and providing the Company with personal data contained in a CV, work-seekers will be giving their consent to processing their details for work-finding purposes. If the Company intends to use their data for any other purpose, it must obtain their specific consent.

Caution is exercised when forwarding personal details of any of the individuals on which data is held to any third party such as past, current or prospective employers; suppliers; customers and clients; persons making an enquiry or complaint and any other third party.

Data in respect of the following is "sensitive personal data" and any information held on any of these matters is not to be passed on to any third party without the express written consent of the individual:

- Any offence committed or alleged to be committed by them
- Proceedings in relation to any offence and any sentence passed
- Physical or mental health or condition
- Racial or ethnic origins
- Sexual life
- Political opinions
- Religious beliefs or beliefs of a similar nature
- Whether someone is a member of a trade union

From a security point of view, only certain named staff are permitted to add, amend or delete data from our databases. However, all staff are responsible for notifying those listed where information is known to be old, inaccurate or out of date.

In addition, all employees should ensure that adequate security measures are in place. For example:

- Computer screens should not be left open by individuals who have access to personal data;
- Passwords should not be disclosed;
- Email should be used with care;
- Personnel files and other personal data should be stored in a place in which any unauthorised attempts to access them will be noticed. They should not be removed from their usual place of storage without good reason;
- Personnel files should always be locked away when not in use and when in use should not be left unattended;
- Any breaches of security should be treated as a disciplinary issue;
- Care should be taken when sending personal data in internal or external mail
- Destroying or disposing of personal data counts as processing, and so care is taken in the disposal of any personal data to ensure that it is appropriate (for example, sensitive data is shredded).

The incorrect processing of personal data e.g. sending an individual's details to the wrong person; allowing unauthorised persons access to personal data; or sending information out for purposes for which the individual did not give their consent, may give rise to a breach of contract and/ or negligence leading to a claim against Foojit for damages from an employee, work-seeker or client contact. A failure to observe the contents of this policy is treated as a disciplinary offence.

Data Security Policy

Data subjects, i.e. those on whom personal data is held, are entitled to obtain access to their data on request and after payment of a fee. All requests to access data by data subjects i.e. staff, members, customers or clients, suppliers, students etc. should be referred to David Peel, Foojit's Operations Director and Data Controller.

Any requests for access to a reference given by a third party must be referred to the administrator and should be treated with caution even if the reference was given in relation to the individual making the request. This is because the person writing the reference also has a right to have their personal details handled in accordance with the Data Protection Act 1998, and not disclosed without their consent. Therefore when taking up references an individual should always be asked to give their consent to the disclosure of the reference to a third party and/or the individual who is the subject of the reference if they make a subject access request. However, if they do not consent, consideration is given as to whether the details of the individual giving the reference can be deleted so that they cannot be identified from the content of the letter. If so, the reference may be disclosed in an anonymous form.

Foojit remains conscious that all individuals have the following rights under the Human Rights Act 1998 and in dealing with personal data these should be respected at all times:

- Right to respect for private and family life [Article 8]
- Freedom of thought, conscience and religion [Article 9]
- Freedom of expression [Article 10]
- Freedom of assembly and association [Article 11]
- Freedom from discrimination [Article 14]

Foojit has put in place the following measures to safeguard personal data of all types:

- All data on internal servers is heavily protected Watchguard technology.
- All inbound/outbound data transfer is made via uncontended, encrypted microwave transmission.
- All laptops are heavily protected and can only be accessed through domain and boot passwords
- All employee details are held as hard copies with duplicates in a fireproof safe. No employee records other than payroll details are held electronically, and Foojit uses logging software when sending information, banking and financial data over TCP/IP.
- No staff may synchronise external devices over the intranet or data storage. Thumb drives, USB sticks and external hard drives are not permitted, and all USB ports are deactivated on static computers.
- All devices and electronic communications are protected by antivirus, spam filters and firewalls.
- We employ external parties (ISO27001 accredited) to test vulnerabilities. This includes periodic blind testing and informed testing after service patch installation in conjunction with vulnerability analysis. These comply with industry standards, ISO/IEC 27001 and our own best practice.
- All employees sign the Postal Services Act and as such adhere to a DPA policy that is unique to postal operators and providers with sanctions in excess of the standard Data Protection Act.
- All employees involved in data handling are security vetted using Scottish Disclosure/CRB checks .