Data Security Policy

Our data security policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data.
It also covers everyday procedures for ensuring good practice in handling, storing and protecting personal and sensitive data.

1. Data Protection Act responsibilities

1.1 We are committed to ensuring that we comply with the eight data protection principles, and meet our legal obligations as laid down by the Data Protection Act 1998. All personal data must be:

a. Processed fairly and lawfully
b. Processed only for one or more specified and lawful purpose
c. Adequate, relevant and not excessive for those purposes
d. Accurate and kept up to date - data subjects have the right to have inaccurate personal data corrected or destroyed if the personal information is inaccurate to any matter of fact
e. Kept for no longer than is necessary for the purposes it is being processed. For example gift aid records need to be kept for six years
f. Processed in line with the rights of individuals - this includes the right to be informed of all the information held about them, to prevent processing of their personal information for marketing purposes, and to compensation if they can prove they have been damaged by a data controller's non-compliance with the Act
g. Secured against accidental loss, destruction or damage and against unauthorised or unlawful processing
h. Not transferred to countries outside the European Economic Area - the EU plus Norway, Iceland and Liechtenstein - that do not have adequate protection for individuals' personal information, unless a condition from Schedule four of the Act can be met.

1.2 Additionally we ensure that:

☐ We will only keep data for the purpose for which it is specifically registered and not disclosed to third parties unless we have specific permission
☐ We take adequate steps to ensure that personal data is up to date and accurate.
☐ Data subjects' rights can be appropriately exercised.
☐ A nominated officer, Ruth Keily, is responsible for data protection compliance and provides a point of contact for all data protection issues.

2. Good practice

2.1 In order to achieve the above, we ensure:

☐ All staff are aware that personal data means any combination of basic information which can be used to identify a person and which could be used e.g. to steal an identity for financial fraud. More sensitive data such as health or family information needs the highest level of care, but even basic information requires protection.

☐ All staff are made aware of good practice in data protection, and that they may be committing a criminal offence and liable to prosecution if they do not adequately protect personal data

☐ Adequate training is provided for all staff responsible for personal data

☐ Everyone handling personal data knows where to find further guidance

☐ Queries about data protection, internal and external to the organisation, are dealt with effectively and promptly

☐ Data protection procedures and guidelines are reviewed at least annually within the organisation.

2.2 Additionally appropriate training is undertaken to ensure staff:
☐ Never disclose personal data to third parties unless authorised to do so

☐ Always ask questions so they can be reasonably assured that the caller is genuine

☐ Establish what information is required - establish whether the caller is entitled to the information, and if in doubt, do not disclose

☐ Be especially cautious if the caller is not the data subject

☐ Never discuss/disclose sensitive information such as medical history.

3. Security measures for personal data
3.1 For hard copy materials a responsible officer ensures that all staff:
☐ Only keep paper copies of materials if strictly necessary e.g. those which have to be collected or referred-to in hard copy during meetings

☐ Maintain a single structured filing system for all staff so that hard copy materials are easily located and kept updated

☐ Keep all materials containing personal data in secure filing storage, which is locked at any time when the office is not staffed

☐ Maintain a clear desk policy with no materials containing personal data left on desks, shelves or filing trays at any time

☐ The door of the office in which hard copy materials are stored is locked out of office hours, with the key being kept only by authorised staff members

☐ Accompany visitors on and off the premises, and do not give any visitor unsupervised access to the computer network or file storage areas

☐ Review files at least annually, and with appropriate authorisation, securely dispose of materials that do not need to be kept or which should be disposed of under point 1.1(e) above.

3.2 For computer security a responsible officer ensures that:
☐ Firewall, virus-checking and anti-spyware software is installed and kept updated on all computers
☐ Computer applications in use on computers are kept updated, with the latest patches or security updates installed to cover vulnerabilities
☐ Staff only access information they need to do their job
☐ Staff use a strong password and do not share passwords with each other. A single master list of network passwords can be accessed with the help of our contracted external IT support agency to ensure business continuity (see below)
☐ Laptops are stored securely when off site, strongly password protected, and never used to store personal data on a local drive
☐ Any personal information held electronically that would cause damage or distress if it were lost or stolen is password protected and/or encrypted
☐ All personal information is removed before disposing of old computers (by using technology or destroying the hard disk).

3.3 To ensure email use does not compromise data security, all staff:
☐ Consider whether the content of the email should be encrypted or password protected.

☐ Take careful note that the correct recipient is addressed

☐ Ensure a recipient whose address should not be revealed to other recipients is blind carbon copied (bcc), not carbon copy (cc).
☐ Are careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.

☐ Only send a sensitive email if you know the recipient's arrangements are secure enough before sending your message

☐ Are aware of the risk of 'phishing' attacks from fraudulent parties asking for any form of personal, password or financial data, their own or others'

☐ Do not open spam messages; delete immediately

☐ Never open attachments from unknown senders or where the attachment from a known sender is not identified or looks in any way suspicious

☐ Do not send or forward emails which could possibly be construed as compromising personal data, being offensive or inappropriate, or risking the reputation of the organisation. Consider all the individuals who may see an email inadvertently (such as children on a shared home computer), not just the immediate addressee.

4. Loss of personal data
4.1 For data security and business continuity in the event of data being lost due to premises or IT damage, we ensure that:
☐ Critical personal data is held on a remote and secure database. Backups of ancillary data are taken on a daily basis.

☐ A master file of business-critical and contact information is maintained where it can be readily accessed in the event of office evacuation, and a copy kept securely offsite

☐ Staff are aware of response procedures in the event of office premises being unusable, including contact numbers and priority actions

☐ In the event of damage to office premises, all materials still stored there are appropriately moved and/or secured as soon as it is safe to access the building.

4.2 In the unlikely event of a data security breach, the following actions are immediately carried out under the direction of a responsible officer:
a. Containment: immediately ensure that no further breaches can occur e.g. by securing hard-copy materials, having IT systems expertly checked for malware, implementing changes and changing passwords.

b. Assessment of the risks: immediately establish what data has been compromised and the specific risks associated with this breach. Evaluate the potential adverse consequences for individuals based on these specifics; how serious or substantial are these risks and how likely they are to happen.

c. Damage limitation: inform those individuals potentially affected (their parents where data affected pertains to under-18s) and ensure they are aware of their need to take appropriate steps such as monitoring communications and changing passwords.

d. Wider notification of breaches: based on the assessed risks, a responsible officer then determines whether it will aid damage limitation if other parties such as the police, other relevant agencies or the media are informed, and implements decisions accordingly.

e. Evaluation and response: investigate the causes of the breach and the effectiveness of the response to it. Update policies and procedures accordingly.