THE BESOM
Sweep away suffering In York

The Besom in York – Data Protection Policy

This data protection policy explains how we store confidential information.

For information on what data we hold and who we hold it on, please see our Privacy Notice on our website.

Information is stored on our Google Drive and Microsoft OneDrive accounts, as well as occasionally on paper in locked storage in our office. Information may be printed out and shared within our organization to facilitate delivery of the service we provide and will be destroyed once the service has been provided.

Network Security

The Besom in York does not have its own network; electronic data is held securely on Google drive and Microsoft OneDrive.

Physical Security

Users should take measures to ensure that paper notebooks or items of electronic equipment holding personal data are reasonably secure. If such devices are portable then extra care is required to prevent theft and to secure sensitive data stored on the device.
When paper copies containing personal data exist they will be securely stored in locked filing cabinets in locked rooms.
Paper copies of files, e.g. delivery schedules, should be returned to the office for secure storage or securely disposed at the end of an activity.
Where documents must be printed to facilitate activities, they should contain the minimum of data necessary for the completion of the activity.

Access Controls

Sensitive data should only be released to trusted users who have read this policy and have been trained in how to secure data. Users must appreciate the potential risks to clients and the organisation.
Users should think carefully about what information to release to other volunteers and only release that which is necessary for the completion of a given activity.

Secure Configuration

Data files or folders containing sensitive personal data must be secured with a strong password. Computers or other electronic devices holding such data should themselves require a secure logon with a suitably strong password or security lock. Try to avoid writing down passwords but if written down they should be kept securely, ideally locked away, and in a location separate from any device that may be accessed using such passwords.

Email & Internet Use

Sharing of personal data over the internet or via email should only take place between trusted users within the organisation. Where files are shared on email or via internet file storage then all such files should be protected with a strong password.
Where password protected files are shared by email, the password for the file should never be sent in the same email.
Personal data should not be sent openly by email.
BCC should be used when sending group emails to protect privacy of email addresses.
For the purpose of keeping statistical records or sharing activities inside or outside of the organisation in the form of – e.g. blogs, newsletters or reports to the Charity Commission – all personal data must be anonymized. Anonymization should not only change names but also not give sufficient information to identify any individual.

Data Storage and Maintenance

Data should not only be stored securely but also maintained and kept accurate. Where there are multiple copies of a file a master copy should be maintained. This copy should be kept up to date and changes/corrections made on other copies must be recorded. Old copies should be regularly deleted and then permanently deleted from Trash.
Data about individual clients should not be kept for longer than is required. This might reasonably be 3 years to allow for follow up contact or further projects. After this period data will be deleted or anonymized to allow for statistical recording of projects and deliveries but not identification of clients.
Data subjects (clients, volunteers, donors, church contacts (including referees) and care professionals) have the right to request their data to be viewed, updated, sent to them in a suitable electronic format or deleted. There is no charge for this service; unless it is manifestly unfounded or excessive. A written (emailed) request must be complied with within 30 days of receipt (see the Privacy Policy).

Management of Breaches

Any breach or potential breach of security should be reported to the trustees. In the result of a serious breach which could result in sensitive data regarding a vulnerable individual being made available to someone who could misuse this to cause harm, e.g. a person seeking a vulnerable person in a refuge, the Care Professional responsible for the vulnerable person's care must be contacted to advise them of the breach. Take measures to contain the breach, e.g. change passwords, and review security arrangements.
Loss of data that is securely protected (e.g. theft of a securely encrypted laptop) does not represent a serious breach.
The trustees will review all data breaches and change policies as appropriate.
All data breaches should be reported upward through the national Besom organisation so that policies and actions can be reviewed and lessons learnt at local and national level. Where appropriate, breaches will be reported to the ICO (Information Commissioner's Office) and individuals whose personal data is involved will be notified.

Training

Trusted data users should be trained in data protection before given access to sensitive data in electronic forms. Volunteers involved in delivering goods and services should be informed and regularly reminded of the importance on maintaining data security and the importance of returning scheduling forms back to data managers especially where vulnerable clients are involved. Trustees should encourage a security aware culture amongst volunteers.

Review

We keep our Data Protection policy under regular review and we will place any updates on this webpage. This privacy policy was last updated on 17/05/2018.