DATA BREACH POLICY

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss or alteration of personal data. It also includes the unauthorised disclosure of, or access to, personal data. A personal data breach can be the result of both accidental and deliberate causes. It is about more than just about losing personal data.

Examples of personal data breaches can include:

- access to the personal data by someone who is not authorised to access it (e.g. personal data being included in a personal email to which someone other than the Foodbank member has access to);
- sending personal data to an incorrect recipient;
- paper copies of personal data or computing devices containing personal data being lost or stolen; and
- alteration of personal data without permission.

There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

What we will do on discovering a data breach?

On discovering a data breach, we will take the following action:

1. We will notify the Data Protection officer, Chair and Secretary of the breach.
2. We will record the data breach on a record of data breaches[1].
3. We will make and record a decision on whether we require to notify the Information Commissioner's Office (ICO) and the Office of the Scottish Charities Regulator (OSCR) of the breach. As required by the Data Protection Act 2018, we will make this decision without undue delay and if feasible, within 72 hours (or as soon as possible thereafter).
4. We will make and record a decision on whether we require to notify the person whose data was the subject of the breach.

[1] This will be stored securely in the Foodbank's Google Drive.

5. We will make and record a decision on whether there is any action that the Foodbank requires to take in order to seek to prevent a similar data breach in the future.

The decisions at 3, 4 and 5 above will be taken by any 2 of the Data Protection Officer, Chair and Secretary. In the event of only one being available, any other trustee can be the additional decision maker. Any action to be considered at 5 above may require the approval of the board.

We will report all data breaches to the board of trustees. This report will include a note of the decisions taken at 3, 4 and 5 above.

What breaches do we need to notify the ICO about?

We will notify the ICO of any personal data breach if it appears that the breach is likely to result in a risk to an individual's rights and freedoms.

A breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage[2].

As required by the Data Protection Act 2018, we will make this decision without undue delay and if feasible, within 72 hours (or as soon as possible thereafter). If we take more than 72 hours to do so, we will provide reasons for the delay.

If we require to notify the ICO of a data breach, we will also notify OSCR of the breach.

[2] For example, if a referral form is mislaid it will be a data breach.
If it is found by a member of the public who then shares that information on social media that is likely to result in considerable risk to the client's rights. Such a breach must be reported to the ICO.
However, if the form is found by another volunteer who keeps the form confidential and returns it to a Board member as soon as possible, that will result in minimal risk to the client's rights. Such a breach will not be reported to the ICO.