Data Protection Policy

Charity registered number 1168176

Introduction

In order to operate efficiently, we must collect information about people with whom we work. These may include members of the public, current, past and prospective employees, funding bodies and suppliers. In addition we may be required by law to collect and use information in order to comply with the requirements of central government.

This personal information must be handled properly under the Data Protection Act 1998 ('the Act'). The Act regulates the way that we handle 'personal data' that we collect in the course of carrying out our functions and gives certain rights to people whose 'personal data' we may hold.

We consider that the correct treatment of personal data is integral to our successful operations and to maintaining trust of the persons we deal with. We fully appreciate the underlying principles of the Act and support and adhere to its provisions.

As a non-profit making charity we are exempted from registration with the Information Commissioner. Nevertheless we abide by the ICO Data protection principles as set out in this policy.

Information covered by the Act

The Act uses the term 'personal data'. For information held by Wycombe Refugee Partnership, personal data essentially means any recorded information held by us and from which a living individual can be identified. It will include a variety of information including names, addresses, telephone numbers, photographs of people and other personal details. It will include any expression of opinion about a living individual or any indication of our intentions about that individual.

Data protection principles

We will comply with the eight enforceable data protection principles by making sure that personal data is:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and kept up to date
- not kept longer than necessary
- processed in accordance with the individual's rights
- secure
- not transferred to countries outside the European Economic area unless the country to which the data is to be transferred has adequate protection for the individuals

Conditions

We will ensure that at least one of the following conditions are met before we process any personal data:

- the individual has consented to the processing
- the processing is necessary for the performance of a contract with the individual
- the processing is required under a legal obligation (other than one imposed by a contract)
- the processing is necessary to protect vital interests of the individual

- the processing is necessary to carry out public functions eg. administration of justice
- the processing is necessary in order to pursue our legitimate interests or those of third parties (unless it could unjustifiably prejudice the interests of the individual)

Under the Act, one of a set of additional conditions must be met for 'sensitive personal data'. This includes information about racial or ethnic origin, political opinions, religious and other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions. We will ensure that one of the following additional conditions are met before we process any sensitive personal data:

- the individual has explicitly consented to the processing
- we are required by law to process the information for employment purposes
- we need to process the information in order to protect the vital interests of the individual or another person
- the processing in necessary to deal with the administration of justice or legal proceedings

Individuals' rights

We will ensure that individuals are given their rights under the Act including:

- the right to obtain their personal information from us except in limited circumstances
- the right to ask us not to process personal data where it causes substantial unwarranted damage to them or anyone else
- the right to claim compensation from us for damage and distress caused by any breach of the Act

Legal requirements

While it is unlikely, Wycombe Refugee Partnership may be required to disclose user data by a court order or to comply with other legal requirements. We will use all reasonable endeavours to notify affected users before we do so, unless we are legally restricted from doing so.

No commercial disposal to third parties

Wycombe Refugee Partnership shall not sell, rent, distribute or otherwise make user data commercially available to any third party, except as described above or with your prior permission.

Our commitment to data protection

We will ensure that:

- everyone managing and handling personal information understands that they are responsible for following good data protection practice
- there is someone with specific responsibility for data protection in the organisation
- staff who handle personal information are appropriately supervised and trained
- queries about handling personal information are promptly and courteously dealt with
- people know how to access their own personal information
- methods of handling personal information are regularly assessed and evaluated
- any disclosure of personal data will be in compliance with approved procedures.
- we take all necessary steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure
- all contractors who are users of personal information supplied by Wycombe Homeless Connection will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by us.

Data Retention guidelines

The Act does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'

This is the fifth data protection principle. In practice, it means that we will:

- regularly review the length of time we keep personal data;
- consider the purpose or purposes for which we hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes;
- and update, archive or securely delete information if it goes out of date.

Data Breach

A data breach is an incident in which personal data is lost, compromised, disclosed to, copied, transmitted, accessed, stolen or used by unauthorised individuals, whether accidentally or on purpose. In the event of a Data Breach the procedures in Appendix 1 should be followed.

Further information

The Information Commissioner – www.informationcommissioner.gov.uk

APPENDIX 1 – Procedures in the event of a Data Breach

1. Introduction

1. WRP holds personal data, both in hard and soft copy, pertaining to clients, volunteers and staff.
2. Care should be taken to protect this type of data, to ensure that it is not changed (either accidentally or deliberately), lost, stolen or falls into the wrong hands, and that its integrity is maintained.
3. In the event of a breach, appropriate action will be taken to minimise associated risks.

2. What is a breach?

2.1. A data breach is an incident in which personal data is lost, compromised, disclosed to, copied, transmitted, accessed, stolen or used by unauthorised individuals, whether accidentally or on purpose. Some examples:

- Accidental loss, theft or failure of equipment on which data is stored
- Unauthorised access to data, such as when a computers are left unattended with confidential information visible
- Human error such as emailing data or verbally mentioning information by mistake
- Hacking attack
- Where information is obtained by deceiving a member of staff

3. Reporting of the breach

3.1. Data security breaches should be reported immediately to the data protection officer. The report should include details of the incident, including who is reporting the incident, what type of data is involved and how many people are affected.

4. Investigation and Risk Assessment

4.1. The data protection officer will establish the nature of the breach, the type of data involved and who are the subjects and how many are involved.

4.2. The investigation will consider the sensitivity of the data, and the risks resulting from the incident.

5. Containment and Recovery

5.1. The data protection officer will determine the appropriate course of action to limit the impact of the breach, such as shutting down critical equipment.

5.2. Appropriate steps will be taken to recover data losses and resume normal operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

6. Notification

6.1. The operations manager and chair of trustees will be notified following a data breach involving large amounts of data, or a significant number of people whose personal data has been breached.

6.2. The data protection officer will inform the Information Commissioner's Office if necessary, based on the extent of the breach.

6.3. Individuals whose data has been compromised will be notified of the nature of the data and of who might have gained access to it within five working days of the discovery of the incident.

6.4. If the data originated with a partner organisation with which WHC has a data sharing agreement, then the partner organisation will be informed in line with the terms of the agreement.

7. Review

7.1. Once the breach is contained a review of the event will be undertaken by the data protection officer and the operations manager to establish the cause of the breach, the effectiveness of the response and to identify areas that require improvement.

7.2. Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

8. Data Protection Officer appointed by the trustees is: Brin Dunsire.

Date: Signed:

Chairman