General Data Protection Regulation
Data Protection Policy

Nottingham Women's Centre
come on in

Nottingham Women's Centre is committed to protecting the security of its information and information systems. It is Nottingham Women's Centre's policy that the information it manages shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to ensure appropriate legal, regulatory and contractual compliance.

We will take steps to guard against the most common causes of data loss or breaches of confidentiality by:

- Making sure that only those who need access to data have that access
- Not storing information where it can be accidentally exposed or lost, e.g. unencrypted USB drives and laptops
- Ensuring that computer systems are appropriately password protected
- Making sure that if data has to be transported it is done so securely using encrypted devices or channels, such as secure email

To determine the appropriate level of security control that should be applied to information systems, a process of risk assessment shall be carried out in order to define security requirements and identify the probability and impact of security breaches.

Purpose

This Data Protection policy defines the framework within which data security will be managed across Nottingham Women's Centre and demonstrates management direction and support for information security throughout Nottingham Women's Centre. This policy is the primary policy under which all other technical and security related polices reside. It should be read in conjunction with the following policies:

- Confidentiality
- Record Keeping
- Child safeguarding
- Adult safeguarding

Scope

This policy is applicable to and will be communicated to all staff, volunteers and other relevant parties. It covers, but is not limited to, any systems or data attached to Nottingham Women's Centre's computer or telephone networks, any systems supplied by Nottingham Women's Centre, any communications sent to or from the Nottingham Women's Centre and any data held on systems external to Nottingham Women's Centre's network.

The principles require that personal information:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met
2. Shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Shall be accurate and, where necessary, kept up to date

5. Shall not be kept for longer than is necessary for that purpose or those purposes
6. Shall be processed in accordance with the rights of data subjects
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Nottingham Women's Centre will, through appropriate management, strict application of criteria and controls:

1. Observe fully, conditions regarding the fair collection and use of information
2. Meet its legal obligations to specify the purposes for which information is used
3. Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
4. Ensure the quality of information used
5. Apply strict checks to determine the length of time information is held
6. Ensure that the rights of people about whom information is held, can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information)
7. Take appropriate technical and organisational security measures to safeguard personal information
8. Ensure that personal information is not transferred without suitable safeguards
9. Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
10. Set out clear procedures for responding to requests for information

In addition, Nottingham Women's Centre will ensure that:

1. There is someone with specific responsibility for Data Protection – this role is held by the Data Controller with support from the Operations Manager
2. Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice, e.g. not leaving women's data on desks unattended
3. Everyone managing and handling personal information is trained to do so and appropriately supervised
4. Anybody wanting to make enquiries about handling personal information knows what to do
5. Queries about handling personal information are dealt with promptly and courteously
6. Methods of handling personal information are clearly described
7. There is a regular review and audit made of the way personal information is held, managed and used
8. Methods of handling personal information are regularly assessed and evaluated
9. Performance with handling personal information is regularly assessed and evaluated
10. Any breach of the rules and procedures identified in this policy by a member of staff is considered a potential disciplinary offence

11. Any breach of the rules and procedures identified in this policy by a volunteer or service user is considered a potential breach of the Code of Conduct

Responsibility

The Board of Trustees are ultimately responsible for the maintenance of this policy and for compliance. This policy has been approved by the Board of Trustees and forms part of its policies and procedures.

The CEO is responsible for the management of information security and, specifically, to provide advice and guidance on the implementation of this policy.

Managers/project coordinators are responsible for identifying and assessing security requirements and risks within their individual projects.

It is the responsibility of all line managers to implement this policy within their area of responsibility and to ensure that all staff/volunteers for which they are responsible are made aware of the policy, and are given appropriate support and resources to comply.

It is the responsibility of each member of staff/volunteer to adhere to this policy.

Breach procedure

Please see Personal Data Breach Policy

Failure to comply with this policy that occurs as a result deliberate, malicious or negligent behaviour, may result in disciplinary action

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the GDPR 2018