DRAFT DATA PROTECTION POLICY

Two key roles we may need to define. If so, will need to decide whether these roles reside within one person or two.

The Controller(s) – ?trustees & manager - says how and why personal data is processed
The Processor – acts on the controller's behalf
Who re us is liable should there be a breach? If I read it right both have key responsibilities – first to ensure contracts reflect GDPR responsibilities and latter to comply with them.

General
Hale Community Centre is fully committed to compliance with the requirements of the Data Protection Act 1998 which came into force on 1 March 2000 and with the the General Data Protection Regulations, which came in to force on 25th May 2018.

The Centre will therefore follow procedures which aim to ensure that all employees and volunteers, and others who have access to any personal data held by or on behalf of the organisation, are fully aware of and abide by their duties under the above.

It is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

1. Statement of policy

In order to operate efficiently, the Centre may be required by law to collect and use information in order to comply with the requirements of central government. All other personal data is held by consent of the data subject or for performance of a contract.

This information and any other personal information collected by us will be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

2. Principles of data protection

The Principles are:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
   a. At least one of the conditions in Schedule 2 is met; and
   b. In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data 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. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.
4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
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. Personal data 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 he processing of personal data.

Do we have a registration number?

1. We shall process personal data in line with all legal requirements and will only process it if at least one of the following is met: (see Schedule 2):

   - Consent of the data subject
   - Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
   - processing is necessary for compliance with a legal obligation
   - processing is necessary to protect the vital interest of a data subject or another person
   - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
   - necessary for the purposes of legitimate interests pursued by the controller or a third party except where such interests are overridden by the interests, rights or freedoms of the data subject.

2. We shall process sensitive personal data (that relating to an individual's health or criminal record) only if at least one of the following conditions prevail: (see Schedule 3):

   a. Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
   b. 9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
   c. 9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

d. 9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
e. 9(2)(e) – Processing relates to personal data manifestly made public by the data subject
f. 9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
g. 9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
h. 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
i. 9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
j. 9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

3. Only personal data that is required and can be justified as required will be processed.

4. We will be transparent at all times (ie fair) in how we intend to use the data and give individuals appropriate privacy notices when collecting their personal data ie information which states who we are, why we need the information and anything else of relevance.

5. All individuals will have right of access to a copy of the personal data held on them by us, a right to have any inaccurate personal data rectified, blocked, erased or destroyed.

6. We will do all we can to ensure the personal data we hold is accurate and, as necessary, kept up to date.

7. No personal data processed for any purpose or purposes shall be kept for longer than is necessary.

8. Appropriate measures (technical and organisational) shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

9. We will not transfer 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.

In addition, we will ensure that: (?)Appendix III 65 V2: 13 August 2012

- there is a named individual with responsibility for data protection within the organisation;
- every member of staff/volunteer responsible for managing and handling personal information, understands that they are contractually responsible for following good data protection practice;
- every member of staff/volunteer responsible for managing and handling personal information, will have access to a copy of this Policy;
- any member of staff or volunteer who has a query about the handling of personal information, knows the relevant person to contact in relation to that query;
- queries from members of the public with respect to the handling of their personal information, are dealt with by staff/volunteers in a prompt and courteous manner and in accordance with the specified time scales set out within the DPA;
- methods of handling personal information are regularly assessed and evaluated;
- where poor handling of personal data by an individual member of staff or volunteer is identified, reasons for such performance will be immediately investigated and determined. Training will then be offered to the member of staff/volunteer to help counteract the problems being experienced by the individual concerned. A further evaluation/assessment should be undertaken within six months, and a log kept of progress made.

The Centre Manager will be responsible for providing support to staff/volunteers with respect to any data protection queries. Any member of staff/volunteer who has a query regarding data protection matters should, in the first instance, contact the Centre Manager.

The administration of Data Protection throughout the organisation will be in accordance with this Policy and relevant operational Procedures. A breach of any of the data protection principles by a member of staff/volunteer is regarded by the Centre as an extremely serious matter. Depending upon the particular circumstances of the breach, such a matter may attract disciplinary proceedings against a member of staff and may be reported to the Police.

This Policy and the relevant operational procedures will be updated on a regular basis in order to reflect any changes within the law; in the event of the Information Commissioner issuing further guidance; or as a result of any reported/apparent ineffective practices or procedures being utilised across the organisation.

The Centre will review its eligibility to be exempt from the requirements to notify the Information Commissioner's Office under the Data Protection Act 1998 (the Act) for ‘not-for-profit’ organisations on an annual basis.

February 2021