

The Centre @ Halton Data Protection Policy

Principles

HCA's Data Protection Policy was drawn up to reflect the UK Data Protection Act 1998 ('the Act') and has been updated to take notice of the General Data Protection Regulation 2016 (GDPR) adopted by the European Union that became effective on May 25, 2018. These regulations have two principal purposes:

- i) To regulate the use by those (known as data controllers) who obtain, hold and process personal data on living individuals, of such personal data; and
- ii) To provide certain rights (for example, of accessing personal information) to those living individuals (known as data subjects) whose data is held.

There are the eight data protection principles, which prescribe:

- i) Guidelines on the information life-cycle (creation/acquisition; holding; processing; querying, amending, editing; disclosure or transfer to third parties; and destruction ('the life-cycle');
- ii) The purpose for which data are gathered and held; and
- iii) Enshrine rights for data subjects.

GDPR applies to **The Centre @ Halton** and to anyone who holds personal information in a structured way so that retrieval is easy. **The Centre @ Halton** is fully committed to abiding, not only by the letter, but also by the spirit of the GDPR, and, in particular, is committed to the observation, wherever possible, of the highest standard of conduct mandated. This policy has been written to acquaint staff and hall hirers with their duties under the GDPR and to set out the standards expected by **The Centre @ Halton** in relation to the processing of personal data and safeguarding individuals' rights and freedoms.

Staff and Hall Hirer duties

Employees and Volunteers of **The Centre @ Halton** are expected to comply with the Data Protection Principles listed below.

The Data Protection Principles

1. Personal data shall be processed fairly and lawfully.
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 they are 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 the GDPR.
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 the processing of personal data.

Those wishing to obtain personal data must comply with guidelines issued from time to time by the Data Protection Officer(DPO) and, in particular, should tell data subjects the purpose(s) for which they are gathering the data, obtain their explicit consent, and inform them that The Centre @ Halton will be the data controller for the purposes of the Act and the identities of any other persons to whom the data may

be disclosed. If sensitive personal data are being collected, explicit consent is not only best practice, it is mandatory. No more data should be collected than is necessary for the purpose(s) declared.

Holding/safeguarding/disposal of personal data

- Data should not be held for longer than is necessary. Personal data should be reviewed periodically to check that they are accurate and up to date and to determine whether retention is still necessary.
- Adequate measures should be taken to safeguard data so as to prevent loss, destruction or unauthorised disclosure. The more sensitive the data, the greater the measures that need to be taken.

Processing of personal data

In the context of GDPR ‘processing’ is defined to include acquisition, passive holding, editing, amending, querying, disclosure and deletion.

Personal data must not be processed except for the purpose(s) for which they were obtained or for a similar, analogous purpose. If the new purpose is very different, the data subject’s consent must be obtained.

Disclosures

The Centre @ Halton’s policy is to exercise its discretion under the GDPR to protect the confidentiality of those whose personal data it holds.

- **The Centre @ Halton** may not disclose any information about any person unless they are clear that they have been given authority by that person to do so. Particular care should be taken in relation to any posting of personal information on the internet.
- **The Centre @ Halton** may not disclose personal data to the police or any other public authority unless that disclosure has been authorised by **The Centre @ Halton’s** DPO.

Transfers

Personal data will not be transferred outside **The Centre @ Halton** except with the data subject’s consent.

Destruction of personal data

Personal data must not be held for longer than necessary; and when such data have been earmarked for destruction, appropriate measures must be taken to ensure that the data cannot be reconstructed and processed by third parties.

Data subjects’ rights of access

The Centre @ Halton is fully committed to facilitating access by data subjects (‘applicants’) to their personal data, while bearing in mind the need to protect other individuals’ rights of privacy. All applicants will be expected to fill in a Subject Access request form.

For the policy regarding CCTV images, please refer to the Data Protection CCTV Policy.

Data Breaches

If a data breach occurs, the DPO must within 72 hours inform the UK data protection authorities of the nature and scope of the breach.

Policy Accepted Date:

Signed:.....

Review Date: