

Data Protection Policy

Wadhurst Institute Hall and Field Trust

Wadhurst Institute Hall & Field Trust is committed to data protection, protecting the rights and freedoms of all those with whom it works, including, but not limited to, employees, trustees and visitors.

Trustees and its employees must recognise the importance of handling personal data appropriately and comply fully with the provisions of the UK General Data Protection Regulation ("the UK GDPR") and the Data Protection Act 2018 ("the DPA").

Scope

This policy and the Data Protection Act apply to all personal data handled by the Trust, whether held in paper format or electronically, where-ever it is held and by whom.

Definitions

'Processing' data is defined as action in relation to data when obtaining, recording, keeping, sharing, disclosing, erasing and destroying such data.

'Personal' data is defined as information relating to a living individual who can be identified from the data

'Special categories of personal data' refers to data that is more sensitive in nature and requires a higher level of protection. This can include an individual's ethnic origin, political opinion, religious beliefs, health trade union membership, sexual orientation, biometric data and criminal convictions.

'Confidential' data is defined as data given in confidence or data agreed to be kept confidential.

Data protection principles

- Process personal data in accordance with the requirements of the Data Protection Act.
- Have a valid, lawful reason to process the data before commencing and obtain/process fairly and lawfully.
- Keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted.
- Keep data up to date.

- Keeps personal data only for the period necessary for processing
- Keep data only that is relevant.
- Process data in a secure manner
- Process 'special category data', ensuring that the individual consents to the data being used and knows what it is being used for, ensuring data is kept and disposed of securely and ensuring that personal data is not disclosed to any unauthorised third party.

Responsibilities of trustees and employees

Report any data found discarded that contains personal data.

Report any data that has been inadvertently disclosed, lost or stolen.

Be mindful that individuals have a right to see their 'personal data'

Ensure data provided is accurate.

Hold data in their possession securely.

Ensure that personal data recorded in paper format or disc/memory stick is held in a locked cupboard/drawer or locked office.

Ensure that any data held on a device is properly password protected.

Ensure special care/ security is undertaken when transferring data.

Breach of policy

Failure to adhere to this policy may constitute a disciplinary offence, which will be dealt with under the ACAS guidelines. Deliberate breaches, including accessing personal data without authorisation or legitimate reason may constitute gross misconduct and lead to dismissal without notice.