



October 2021

Access to Employee Data — GDPR Policy

The organisation aims to fulfil its obligations under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 to the fullest extent.

Personal data may include information held in manual files, on the organisation's computer system, in emails, mobile phones or on CCTV footage.

The organisation endorses fully and adheres to the six principles of data protection as set out in the Article 5 of GDPR.

1. Data will be processed lawfully, fairly and in a transparent manner.
2. Data will be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.
3. Data will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
4. Data will be accurate and, where necessary, kept up to date.
5. Data will be kept for no longer than is necessary for the purposes for which it was collected.
6. Data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Employees whose roles involve access to personal data must follow these principles at all times when processing or using employees' personal information.

Data Security

All employees whose roles involve access to personal data are responsible for ensuring that the data they hold is kept securely and that it is not disclosed, whether accidentally or otherwise, to any unauthorised third party.

Personal information should be kept in a locked filing cabinet, drawer or safe. If it is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer or safe.

Any unauthorised disclosure will normally be regarded as a disciplinary matter, and may be considered gross misconduct in some cases.

Access to Personal Data

1. All employees are responsible for ensuring that the personal data they provide to the organisation is complete, accurate and up-to-date. Any changes to information, eg changes of address, must be notified promptly to Laura Foster, Shellie Prager or Rachael Smith.
2. Employees have the right to access their personal data at reasonable intervals. The organisation believes that complying with a request for a copy of the data annually will satisfy this requirement.
3. If an employee wishes to request access to their personal data, the request must be in writing and addressed to Laura Foster. The request should, as far as possible, specify what information the employee is seeking.
4. In the event of a reasonable written request for access, the information requested will be provided without delay and at the latest within one month of receipt of the request.
5. Employees should inform Julie Partridge or Laura Foster at the earliest opportunity if they believe that any of their personal data is inaccurate or untrue, or if they are dissatisfied with the information in any way.
6. In the event of a disagreement between an employee and the organisation regarding personal data, the matter should be taken up under the organisation's formal grievance procedure.

Additional Clause(s)

1. In line with the guidance from the Information Commissioner's Office on GDPR, requests to access employee's data by the employee concerned will not normally be charged for. However, it is permissible, where an employee makes a request for access to their personal data which is manifestly unfounded or excessive, particularly when requests are repetitive, a reasonable fee of £30 can be charged. This must be paid to Laura Foster before a copy of the personal data will be given. The fee is based on the administrative cost of providing the information.
2. In the interests of openness and fairness, the organisation will provide copies of personal records held manually to employees when asked in January each year. This will be done proactively and at no cost to the employee.