

DATA PROTECTION POLICY

The Company, within the UK, is registered as a data user in accordance with the terms of the UK Data Protection legislation in force from time to time and there are procedures in place to ensure compliance with that legislation. The Company will need to hold certain data about you in its capacity as your Employer.

This data held may include personal data consisting of the following information: racial or ethnic origin, trade union membership, your physical and mental health or condition, the commission or alleged commission by you of any offence or any proceedings for any offence committed or alleged to have been committed by you. The disposal of such proceedings or the sentence of any proceedings or the sentence of any court in such proceedings.

We are required to provide your personal data to outside Organisations to allow us to administer your employment and benefits package effectively. This currently includes but may not be limited to Central Government (taxation), Insurance (includes Healthcare, Permanent Health Insurance, Life Assurance) and Pension providers.

Any information held will be processed at all times in accordance with the data protection principles set out in the Data Protection Act 1998.

In the course of your employment, you will be expected to comply with the requirements of the Data Protection Act 1998 and the Company Policy relating to the fair processing of personal data.

By signing this agreement you consent to the Company obtaining, recording and using information about yourself, in connection with your employment and for so long after your employment as may be reasonably required for the legitimate purposes of the Company. (For example, we require your name, address, bank details in order to be able to pay you).

Accepting these terms and conditions of employment indicates your consent to these procedures.

Policy Statement

Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our employees and we recognise the need to treat it in an appropriate and lawful manner.

The types of information that we may be required to handle include details of current, past and prospective employees, Trustee Board Members, volunteers, contractors (including Tutors), members of the public and others that we communicate with.

The information, which may be held on paper or on a computer or other media source, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations. The Act imposes restrictions on how we may use that information.

Status of the Policy

This sets out our rules on data protection and the legal conditions that must be satisfied in relation to obtaining, handling, processing, storage, transportation and destruction of personal information.

The Data Protection Compliance Manager is responsible for ensuring compliance with the Act. Any questions or concerns about the operation should be referred in the first instance to the Data Protection Compliance Manager.

Employees who consider that our provisions for complying with the Act have not been followed in respect of personal data about themselves or others they should raise the matter with their Line Manager or the Data Protection Compliance Manager.

Definition of Data Protection Terms

- Data is information which is stored electronically on a computer or in certain paper based filing systems.
- Data Subjects for this purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.
- Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).
- Data controllers are the people who or organisations which determine the purposes for which, and the manner in which any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.
- Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.
- Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.
- Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
- Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate.

- Not kept longer than necessary for the purpose.
- Processed in line with data subject's rights.
- Secure
- Not transferred to people or organisations situated in countries without adequate protection.

Fair and Lawful Processing

The act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is, in this case Rotunda Limited and the data controllers representative is, in this case the Data Protection Compliance Manager, the purpose for which the data is to be processed by us and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subjects explicit consent to the processing of such data will be required.

Processing for Limited Purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any purposes specifically permitted by the Act. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

Adequate, Relevant and Non-Excessive Processing

Personal data should only be collected to the extent that it is required for the specific purposes notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

Accurate Data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

Timely Processing

Personal data should not be kept longer than is necessary for the purpose it is intended. This means that data should be destroyed or erased from our systems when it is no longer required. For guidance on how long certain data is likely to be kept before being destroyed contact the Data Protection Compliance Manager or your Line Manager.

Processing in Line with Data Subject's Rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any data held about them by a data controller.
- Prevent the processing of their data for direct marketing purposes.
- Ask to have inaccurate data amended.

- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Data Security

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third party data processor if he/she agrees to comply with those procedures and policies, or if he/she puts in place adequate measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures include:

- Entry controls. Any stranger seen in entry controlled areas should be reported.
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential).
- Methods of disposal. Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.
- Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

Dealing with Subject Access Requests

A formal request from a data subject for information that we hold about them must be made in writing. A fee is payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to their Line Manager or the Data Protection Compliance Manager immediately.

Providing Information over the Telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

- Check the caller's identity to ensure that the information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
- Refer to their Line Manager or the Data Protection Compliance Manager for assistance in difficult situations. No one should be bullied into disclosing personal information.

Company personnel individual files policy.

The Company policy with regard to individual's personal files which applies under the Data Protection Act, all information electronic or hard copy will be placed on the personnel file of each individual employee.

Any employee requesting access to any or all information held on their own individual personal file must make a request to a Senior Manager, that request must be in writing and approval is required from the Chief Executive Officer or their nominated deputy.

Individual's private personal files will only be released when a written application has been made and provision of the file has been approved by the Senior Manager and the CEO or their nominated deputy.

The file physically will be provided to the individual employee, this is in order to allow the employee to read the contents whilst on the company premises. If any copies of documents on the file are requested those documents will be copied and provided to the individual employee on the strict understanding that the contents of the file will not to be removed from the Company premises.

Photocopies will be provided upon request by completion of an appropriate request form stating the documents which the individual employee has requested to be photocopied and given to them.

Rotunda Policy Review Record

Reviewed by:	Approval date:	Review frequency:	Review date:	Signed:
Maxine Ennis	18 th January 2024	Annual	18 th January 2025	