Data Protection Policy

Contents

1. Aims and Objectives

The aim of this policy is to ensure that when processing information about individuals we comply with the eight data protection principles as laid down by the Data Protection Act 1998.

The data protection principles reflect good practice in the handling of personal information, therefore the purpose of this policy is to ensure that:

a. We have individuals' consent to the holding of information about them;
b. The information is used only for the purposes for which it was obtained;
c. The information is accurate and retained only for so long as is necessary; and
d. The information is not passed on to anyone else without the individuals consent.

We take a zero-tolerance approach to data protection and are committed to adhering to the Data Protection Act 1998 in all our business dealings and relationships wherever we operate and implementing and enforcing effective systems.

We will uphold all laws relevant to data protection in all the jurisdictions in which we operate. However, we remain bound by the laws of the UK, including the Data Protection Act 1998, in respect of our conduct both at home and abroad.

Incorrect processing of personal data and failure to comply with the Data Protection Act may give rise to a breach of contract and/or negligence leading to a claim against us for damages from an employee, work-seeker or client contact. Failure to observe the contents of this policy will be treated as a disciplinary offence under ***The RTC Group Disciplinary Procedure.***

2. Status of this Policy

This policy applies to you:

a) as an employee of The RTC Group and subsidiary companies; and
b) as a representative of The RTC Group PLC and subsidiary companies

Therefore you are both protected by this policy and are also required to adhere to the Data Protection Principles during your daily working activities (also see ***Data Protection Policy – Recruitment***).

This policy is designed to protect all individuals. The term **individual** means any living individual you come into contact with during the course of your work for us and includes, but is not limited to:

- Current and former employees
- Contractors or agency workers
- Job Applicants
- Customers

This procedure does not give contractual rights to individual employees, workers or contractors. The company reserves the right to alter any of its terms at any time although we will notify you of any changes and upload an updated version to the Company Intranet.

3. Data Protection Principles

The Data Protection Act controls how personal information is used by organisations, businesses and the Government and anyone who is responsible for using data has to follow the eight data protection principles to ensure that the information is:

1. Used fairly and lawfully
2. Used for limited, specifically stated purposes
3. Used in a way that is adequate, relevant and not excessive
4. Accurate
5. Not kept longer than absolutely necessary
6. Handled according to people's data protection rights
7. Kept safe and secure
8. Not transferred outside the UK without adequate protection

In addition there is a stronger legal protection for more sensitive information, including:

- Ethnic background
- Political opinions
- Religious beliefs
- Health

- Sexual health
- Criminal records

4. Processing

The term **processing** covers all forms of handling information, including:

- Obtaining and recording it
- Using and manipulating it
- Holding it and
- Passing it on

5. Personal Information

In order to be covered by the legislation, the information must be 'personal information'. Information is not personal simply because it names an individual or records that the individual was involved in an event with no personal connotations. Information will however be covered if it consists of personal details about the individual and has the individual as its focus.

The Act covers information held both electronically and manually and therefore the data protection principles should be observed in relation to:

- Application forms
- Recruitment documentation (interview notes, assessments etc.)
- Personal details (address, contact details, date of birth etc.)
- Payroll information
- Equal opportunities monitoring forms
- Medical records
- Sickness absence records
- Attendance records
- Records of Disciplinary/Grievance proceedings
- Personnel files relating to former employees

6. Used fairly and lawfully

The first data protection principle is that information must be processed fairly and lawfully and in accordance with at least one of the following conditions:

- The individual has consented to the processing.
- The processing is necessary for the performance of the individual's employment contract or in order to enter into an employment contract with the individual. This could apply, for example, to the processing of information given on a job application form.
- The processing is necessary for the employer to comply with a legal obligation, other than a contractual obligation. For example, this could cover processing that is necessary in order for the employer to deduct income tax from an employee's pay.
- The processing is necessary to protect the vital interests of the individual. This covers life and death situations, such as where an employer may need to give information about an individual's medical history to a hospital if he or she has had an accident at work.

- The processing is necessary for the purposes of the employer's legitimate interests and does not unduly prejudice the individual. This broadly phrased condition will cover many types of processing that a company must carry out in the course of employing an individual.

Where the information is sensitive information (as per section 4) then additional requirements must be imposed and one of the above conditions must be met in addition to one of the following additional conditions:

- The individual has given his or her explicit consent to the processing.
- The processing is necessary in order for the employer to exercise or perform any legal right or obligation connected with employment.
- The processing is necessary to protect the vital interests of the individual or another person, and the individual cannot give consent or the employer cannot reasonably be expected to obtain the individual's consent.
- The processing is necessary for the purposes of legal proceedings.
- The processing is necessary for medical purposes, provided it is undertaken by a health professional or someone who owes a similar duty of confidentiality.
- Where the processing relates to information about an individual's racial or ethnic origin, religious beliefs or physical or mental condition, the processing is necessary to monitor equal opportunities.

In order for the information to be processed fairly, you must provide the individual with certain information at the time the information is obtained, including:

- The identity of the employer;
- If the employer has nominated a representative for the purposes of meeting the requirements of the Act, the identity of that person;
- The purposes for which the information is intended to be processed;
- The likely consequences of the processing;
- Whether the employer anticipates that it will disclose the information to anyone else.
- Processing for a specified purpose

7. Used for limited, specifically stated purposes

The second data protection principle is that information must be obtained only for a specified purpose, and must then be dealt with in a way that is compatible with that purpose.

The individual should have been notified of the purpose for which the information was to be held when it was first obtained (as per section 8).

This principle means, for example, that an employer who has obtained an employee's home address for the purpose of personnel administration should not then use that address for marketing purposes.

8. Used in a way that is adequate, relevant and not excessive

The third data protection principle is that you must ensure that the information you obtain and hold is relevant for the purpose for which it was intended. It must be full enough to meet that purpose but must not be excessive.

9. Accurate

The fourth data protection principle requires that information should be accurate and kept up to date.

It is therefore important that we have a system in place to check the accuracy of personal information periodically. We cannot be held accountable for any inaccuracies in information supplied by the individual or a third party, providing we have taken reasonable steps to ensure the accuracy of the information.

In addition, it is your responsibility to ensure that the information we hold on you as an employee is up to date and any changes to such information is communication in a timely manner to The Group HR Department.

10. Not kept longer than absolutely necessary

Under the fifth data protection principle, you should ensure that you do not retain information for any longer than you need to in order to meet the purpose for which it was held.

For example, employers will need to establish a system for reviewing the information they hold on ex-employees, to ensure that the information is kept only for as long as is necessary to cater for specific purposes. An example of this might be the possibility of needing to defend a legal action or satisfy the Inland Revenue that the correct tax deductions were made.

11. Handled according to people's data protection rights

The sixth data protection principle is that you must ensure that, in processing information about individuals, you observe the rights those individuals have under the Act.

These rights include an individual's right to have access to the information that is held on them (as per section 15 and 16)

12. Kept safe and secure

Under the seventh data protection principle, you must take steps to ensure that personal information is not processed in an unauthorised or unlawful way, and is not lost, destroyed or damaged.

If you have access to personal information, you must be aware of your responsibility to keep the information confidential and not to disclose it in an unauthorised way.

In order to protect this information you must ensure that adequate security measures are in place, including but not limited to:

- Locking computer screens when away from your desk;
- Regularly changing and not disclosing your password;
- Keeping personal information locked away securely, i.e. Personnel files should be stored in a lockable filing cabinet;
- Taking care when sending personal information via post and email;
- Securely destroying personal information.

Please see the ***RTC Group Electronic Communications Policy.***

13. Not transferred outside the UK without adequate protection

Under the eighth data protection principle, if you are required to transfer personal information outside the European Economic Area, it must ensure that the country to which the information is transferred has adequate data protection measures in place. This principle does not apply if the individual has consented to the transfer of the information or if the transfer is necessary for the performance of the individual's employment contract.

14. Subject Access Rights

The Data Protection Act gives various rights to individuals whose personal information is processed. One of the most important is the right to know what information an employer/organisation holds on them.

In order to have access to this information, an individual must make a request in writing allowing the employer/organisation 40 days to comply with the request and is entitled to ask for a fee of up to £10.

For further information on Subject Access Requests or to make one please contact The Group HR Department.

14.1. Exemptions from disclosure

An employer/organisation does not have to disclose information that includes information about another individual or that identifies a particular person as the source of the information, unless the other person consents to the disclosure, or it is reasonable in all the circumstances to comply with the request without the other person's consent.

For example, we need not disclose to you any confidential reference received from a current or former employer.

In addition an employer/organisation need not disclose information that is processed for the purposes of management forecasting or management planning, if that would be likely to prejudice the conduct of the business.

15. Automated decision-making

The Data Protection Act gives individuals certain rights if a decision is made about them on an automated basis. An automated decision would include, for example, a decision on whether to offer an individual a job interview based solely on automatic CV scanning. The employer/organisation must inform the individual when an automated decision has been made.

On the individual's written request, the employer/organisation must provide a written explanation of the logic involved in the decision-making process. Further, it must take steps to safeguard the individual's interests by, for example, allowing him or her to make representations about the way in which the decision was reached.

16. Failure to comply

You must remember that the incorrect processing of personal information, i.e. sending personal information to the wrong person, allowing unauthorised personal access or using the personal information for purposes other than what it was originally obtained for may give rise to a claim against The RTC Group as below (see 16.1, 16.2 and 16.3) and therefore failure to comply with The Data Protection Act and the content of this policy could invoke action under the ***RTC Group Disciplinary Procedure***.

16.1. Enforcement

If we contravene the data protection principles and an individual suffers damage or damage and distress as a result, he or she can apply to a court for compensation. We have a defense to the claim if we can show that we took such care as was reasonable in all the circumstances to comply with the Act.

16.2. Court order

A court can also order an employer/organisation to correct, block, erase or destroy information that is inaccurate, or which contains an expression of opinion that is based on inaccurate information.

An order of this type can also be made if the individual has suffered damage because the employer/organisation has failed to comply with the data protection principles and the court considers that there is a substantial risk that further contraventions of the Act will occur.

16.3. Enforcement Notice

An individual may also ask the Information Commissioner to assess whether the employer/organisation is complying with the Act. Depending on the result of that assessment, the Commissioner may decide to bring enforcement action against the employer/organisation. The Commissioner has the power to serve an enforcement notice on an employer/organisation, requiring it to comply with the Act. Failure to comply with an enforcement notice is a criminal offence, unless the employer/organisation can show that it exercised all due care to comply.

17. Information Commissioner

Organisations that process personal information by computer may have to notify the Information Commissioner, so that their details can be entered in a public register.

A small fee is payable for notification of Data Controllers and notification must be renewed annually.

An organisation has no duty to notify if it processes personal information only for one or more of these purposes:

- staff administration;
- advertising;
- marketing and public relations; or
- accounts and records.

18. Compliance Checklist

In order to ensure that you comply with the data protection principles, you must consider the following steps:

- Consider what personal information is currently held, for what purposes and by whom.
- Assess whether the way information is currently processed complies with the data protection principles.
- Consider whether consent is needed in order to process any personal information that the company holds, and if it is, how consent should be obtained.
- Identify and mark sensitive information.
- Ensure that the company has adequate arrangements to keep personal information secure (safeguarding information).
- Ensure that outdated, inaccurate and irrelevant information (obsolete information) is disposed of.
- If information is sent outside the EEA, whether consent is required to do so.
- Consider putting in place a procedure for dealing with subject access requests (subject access rights).

If you have any queries relating to this policy or enquiries or complaints please contact The Group HR Department.

19. Related Policies

- ***RTC Group Disciplinary Procedure***
- ***Data Protection Policy - Recruitment***
- ***RTC Group Electronic Communications Policy***