



GDPR Data Protection Policy & Employee Data Procedure

Data Protection Policy Statement

Farol is fully committed to full compliance with the requirements of the Data Protection Act 2018. The company will therefore follow procedures which aim to ensure that all employees, contractors, consultants, (collectively known as data users) who have access to any personal data held by or on behalf of the company are fully aware of and abide by their duties under the Act.

Statement of Policy

The company needs to collect and use information about people with whom it works to operate and carry out its functions. These may include current, past and prospective employees, and customers and suppliers. This personal information must be handled and dealt with properly however it is collected, recorded and used and whether it is on paper, in computer records or recorded by other means.

For employment purposes these records may include:

- information gathered about an employee and any references obtained during recruitment
- details of terms of employment
- payroll, tax and National Insurance information
- performance information
- details of grade and job duties
- health records
- absence records, including holiday records and self-certification forms
- details of any disciplinary investigations and proceedings
- training records
- contact names and addresses
- correspondence with the Organisation and other information provided to the Organisation.

Farol Ltd believes these uses are consistent with our employment relationship and with the principles of the DPA. The information held will be for our management and administrative use only, but from time to time, we may need to disclose some information we hold about employees to relevant third parties. We may also transfer information to another group or Organisation, solely for purposes connected with an employee's career or the management of the Organisation's business.

It should also be noted that the Organisation might hold the following information about an employee for which disclosure to any person will be made only when strictly necessary for the purposes set out below:

- an employee's health, for the purposes of compliance with our health and safety and our occupational health obligations
- for the purposes of HR management and administration, for example to consider how an employee's health affects his or her ability to do his or her job and, if the employee is disabled, whether he or she requires any reasonable adjustment to be made to assist him or her at work
- the administration of insurance, pension, sick pay and any other related benefits
- in connection with unspent convictions to enable us to assess an employee's suitability for employment.

Farol Ltd regards the lawful and appropriate treatment of personal information as very important to its successful operations and essential to maintaining confidence between the company, all employees and those with whom it carries out business. The company therefore fully endorses and adheres to the Principles of the Data Protection Act.

Farol Ltd requires all employees to comply with the Data Protection Act in relation to the information about other staff and customers. Failure to do so will be regarded as serious misconduct and will be dealt with in accordance with the Organisation's disciplinary policy and procedure. If an employee is in a position to deal with personal information about other employees, he or she will be given separate guidance on his or her obligations, and must ask if he or she is unsure.

Handling personal/sensitive data

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage
- securely destroy data which is no longer needed

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

We will ensure that the company has a Director (Matt Balch) and an employee (Jo Robinson) specifically responsible for data protection.

Your Rights

These include the right to:

- be informed about how your data is being used
- the right to access your own personal information. Formal requests should be made to the HR Director (Ali Anning). We charge a fee each time a formal request for information is made by an employee. This is currently £10.
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data in certain circumstances
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

The Principles of Data Protection

The DPA 2018 has also adopted the seven principles of the GDPR and, as a business owner or decision maker. These Principles are legally enforceable.

Summarised, the principles require that personal data :

1. Shall be processed lawfully, fairly and transparently and in particular, shall not be processed unless specific conditions are met;
2. 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. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed (data minimisation);
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be kept secure i.e. protected by an appropriate degree of security;
7. Accountability – to take responsibility for the processing activities we carry out. To ensure on-going compliance, every step of the GDPR strategy must be auditable through the use of our policies and procedures.

Your duties to assist in the correct handling of Data

To help us keep accurate information, you must tell us about changes to your contact or payroll details. If you know that we hold any other personal details about you that are out of date or inaccurate you must tell us.

You also have a role to play in helping us meet our obligations to handle personal data relating to other employees in accordance with the Act.

If you receive a request for disclosure of information about another employee from someone not employed by us, you must be careful. You should take all reasonable steps to establish the identity of the person seeking the information, obtain a written request or phone number and then pass the request to the HR Director.

If you need to handle personal information relating to another employee as part of your job, you should do so only as reasonably necessary for your job and take all reasonable steps to protect the security of that information.

If you have managerial responsibility for staff, you should be careful when collecting records about your staff or department. You must do so only as reasonably necessary for management purposes and must take all reasonable steps to protect the security of that information. If you are asked to give a reference about a current or previous employee, you should seek approval of the wording from the

HR Director before sending it. You are not prevented from providing references in a personal capacity, but we will not have any responsibility for the information in that reference.

Anyone in any doubt about handling personal information relating to other employees should seek guidance. Accessing, keeping, disclosing or otherwise using records of other employees without authority is a serious disciplinary offence (and in some cases may constitute a criminal offence).



Signed:

Ali Anning; HR Business Partner

Last reviewed 18/05/2023