



EMPLOYEE DATA POLICY

This document sets out the Galleon Centre's policy on the protection of information relating to staff members, workers, contractors, volunteers and interns (referred to as staff members). Protecting the confidentiality and integrity of personal data is a critical responsibility that the Galleon Centre takes seriously at all times. The Galleon Centre will ensure that data is always processed in accordance with the provisions of relevant data protection legislation, including the General Data Protection Regulation (GDPR).

KEY DEFINITIONS

Data processing

Data processing is any activity that involves the use of personal 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 transmitting or transferring personal data to third parties.

Personal data

Personal data is any information identifying a data subject (a living person to whom the data relates). It includes information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers the Galleon Centre possesses or can reasonably access. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Sensitive personal data

Sensitive personal data is a special category of information which relates to a data subject's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. It also includes personal data relating to criminal offences and convictions.

PRIVACY NOTICE

This policy, together with the information contained in the table of staff member data appended to the policy, constitutes a privacy notice setting out the information the Galleon Centre holds about staff members, the purpose for which this data is held and the lawful basis on which it is held. The Galleon Centre may process personal information without staff members' knowledge or consent, in compliance with this policy, where this is required or permitted by law.

If the purpose for processing any piece of data about staff members should change, the Galleon Centre will update the table of staff member data with the new purpose and the lawful basis for processing the data and will notify staff members.

FAIR PROCESSING OF DATA

Fair processing principles

In processing staff members' data the following principles will be adhered to. Personal data will be:

- Used lawfully, fairly and in a transparent way;
- Collected only for valid purposes that are clearly explained and not used in any way that is incompatible with those purposes;
- Relevant to specific purposes and limited only to those purposes;
- Accurate and kept up to date;
- Kept only as long as necessary for the specified purposes; and
- Kept securely.

Lawful processing of personal data

Personal information will only be processed when there is a lawful basis for doing so. Most commonly, the Galleon Centre will use personal information in the following circumstances:

- when it is needed to perform staff member' contracts of employment;
- when it is needed to comply with a legal obligation; or
- when it is necessary for the Galleon Centre's legitimate interests (or those of a third party) and staff members' interests and fundamental rights do not override those interests.

The Galleon Centre may also use personal information in the following situations, which are likely to be rare:

- when it is necessary to protect staff members' interests (or someone else's interests); or
- when it is necessary in the public interest or for official purposes.

Lawful processing of sensitive personal data

The Galleon Centre may process special categories of personal information in the following circumstances:

- In limited circumstances, with explicit written consent;
- in order to meet legal obligations;
- when it is needed in the public interest, such as for equal opportunities monitoring or in relation to the Galleon Centre's occupational pension scheme; or
- when it is needed to assess working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, the Galleon Centre may process this type of information where it is needed in relation to legal claims or where it is needed to protect any staff members interests (or someone else's interests) and the staff member is not capable of giving consent, or where a staff member has already made the information public. The Galleon Centre may use particularly sensitive personal information in the following ways:

- information relating to leaves of absence, which may include sickness absence or family related leaves, may be used to comply with employment and other laws;

- information about staff members physical or mental health, or disability status, may be used to ensure health and safety in the workplace and to assess fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits;
- information about race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, may be used to ensure meaningful equal opportunity monitoring and reporting; and
- information about trade union membership may be used to pay trade union premiums, register the status of a protected staff member and to comply with employment law obligations.

Lawful processing of information about criminal convictions

The Galleon Centre envisages that it will hold information about criminal convictions. If it becomes necessary to do so, the Galleon Centre will only use this information where it has a legal basis for processing the information. This will usually be where such processing is necessary to carry out the Galleon Centre's obligations. Less commonly, the Galleon Centre may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect a staff members interests (or someone else's interests) and the staff member is not capable of giving consent, or where the staff member has already made the information public.

Where appropriate, the Galleon Centre will collect information about criminal convictions as part of the recruitment process or may require staff members to disclose information about criminal convictions during the course of employment.

Consent to data processing

The Galleon Centre does not require consent from staff members to process most types of staff member data. In addition, the Galleon Centre will not usually need consent to use special categories of personal information in order to carry out legal obligations or exercise specific rights in the field of employment law. If a staff member fails to provide certain information when requested, the Galleon Centre may not be able to perform the contract entered into with the staff member (such as paying the staff member or providing a benefit). The Galleon Centre may also be prevented from complying with legal obligations (such as to ensure the health and safety of staff members).

In limited circumstances, for example, if a medical report is sought for the purposes of managing sickness absence, staff members may be asked for written permission to process sensitive data. In those circumstances, staff members will be provided with full details of the information that is required and the reason it is needed, so that staff members can carefully consider whether to consent. It is not a condition of staff members contracts that staff members agree to any request for consent.

Where staff members have provided consent to the collection, processing and transfer of personal information for a specific purpose, they have the right to withdraw consent for that specific processing at any time. Once the Galleon Centre has received notification of withdrawal of consent it will no longer process information for the purpose or purposes originally agreed to, unless it has another legitimate basis for doing so in law.

Automated decision making

The Galleon Centre does not envisage that any decisions will be taken about staff members using automated means, however staff members will be notified if this position changes.

COLLECTION AND RETENTION OF DATA

Collection of data

The Galleon Centre will collect personal information about staff members through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. The Galleon Centre may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies such as Disclosure Scotland.

The table of staff member data appended to this policy relates to information which is collected at the outset of employment. From time to time, the Galleon Centre may collect additional personal information from individuals in the course of job-related activities throughout the period of employment. If the Galleon Centre requires to obtain additional personal information this policy will be updated or staff members will receive a separate privacy notice setting out the purpose and lawful basis for processing the data.

Retention of data

The Galleon Centre will only retain staff members personal information for as long as necessary to fulfil the purposes it was collected for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of personal information are set out in the table of staff member data appended to this policy.

When determining the appropriate retention period for personal data, the Galleon Centre will consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of personal data, the purposes for which the personal data is processed, whether the Galleon Centre can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances the Galleon Centre may anonymise personal information so that it can no longer be associated with individual staff members, in which case the Galleon Centre may use such information without further notice to staff members. After the data retention period has expired, the Galleon Centre will securely destroy staff members personal information.

DATA SECURITY AND SHARING

Data security

The Galleon Centre has put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Details of these measures are available upon request. [Access to personal information is limited to those staff members, agents, contractors and other third parties who have a business need to know. They will only process personal information on the

Galleon Centre's instructions and are subject to a duty of confidentiality.] The Galleon Centre expects staff members handling personal data to take steps to safeguard personal data of staff members (or any other individual) in line with this policy.

Data sharing

The Galleon Centre requires third parties to respect the security of staff member data and to treat it in accordance with the law. The Galleon Centre may share personal information with third parties for example in the context of the possible sale or restructuring of the business. The Galleon Centre may also need to share personal information with a regulator or to otherwise comply with the law.

The Galleon Centre may also share staff member data with third-party service providers where it is necessary to administer the working relationship with staff members or where the Galleon Centre has a legitimate interest in doing so.

STAFF MEMBER RIGHTS AND OBLIGATIONS

Accuracy of data

The Galleon Centre will conduct regular reviews of the information held by it to ensure the relevancy of the information it holds. Staff members are under a duty to inform the Galleon Centre of any changes to their current circumstances. Where a staff member has concerns regarding the accuracy of personal data held by the Galleon Centre, the staff member should contact the Deputy General Manager to request an amendment to the data.

Applicant rights

Under certain circumstances, staff members have the right to:

- **Request access** to personal information (commonly known as a “data subject access request”).
- **Request erasure** of personal information.
- **Object to processing** of personal information where the Galleon Centre is relying on a legitimate interest (or those of a third party) to lawfully process it.
- **Request the restriction of processing** of personal information.
- **Request the transfer** of personal information to another party.

If any staff member wishes to make a request on any of the above grounds, they should contact the Deputy General Manager in writing. Please note that, depending on the nature of the request, the Galleon Centre may have good grounds for refusing to comply. If that is the case, the staff member will be given an explanation by the Galleon Centre.

Data subject access requests

Staff members will not normally have to pay a fee to access personal information (or to exercise any of the other rights). However, the Galleon Centre may charge a reasonable fee if the request for access is clearly unfounded or excessive. Alternatively, the Galleon Centre may refuse to comply with the request in such circumstances.

The Galleon Centre may need to request specific information from the staff member to help confirm their identity and ensure the right to access the information (or to exercise any of the other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

COMPLIANCE WITH THIS POLICY

The Galleon Centre's responsibility for compliance

The Kilmarnock Leisure Centre Trust is tasked with overseeing compliance with this policy. If staff members have any questions about this policy or how the Galleon Centre handles personal information, they should contact the Deputy General Manager. Staff members have the right to make a complaint at any time to the Information Commissioner Office (ICO), the UK supervisory authority for data protection issues.

Data security breaches

The Galleon Centre has put in place procedures to deal with any data security breach and will notify staff members and any applicable regulator of a suspected breach where legally required to do so. Details of these measures are available upon request.

In certain circumstances, the Galleon Centre will be required to notify regulators of a data security breach within 72 hours of the breach. Therefore, if a staff member becomes aware of a data security breach it is imperative that they report it to the Deputy General Manager immediately.

Privacy by design

The Galleon Centre will have regard to the principles of this policy and relevant legislation when designing or implementing new systems or processes (known as "privacy by design").

Staff members' responsibility for compliance

All staff members, particularly those tasked with regularly handling personal data of colleagues or third parties, have responsibility for ensuring that processing meets the standards set out in this policy. Staff members should observe, as a minimum, the following rules:

- Staff members must observe to the letter any instruction or guidelines issued by the Galleon Centre in relation to data protection.
- Staff members should not disclose personal data about the Galleon Centre, colleague or third parties unless that disclosure is fair and lawful, in line with this policy;
- Staff members must take confidentiality and security seriously, whether the staff member considers the information to be sensitive or not.
- Any personal data collected or recorded manually which is to be input to an electronic system should be input accurately and without delay.
- Staff members must not make any oral or written reference to personal data held by the Galleon Centre about any individual except to staff members of the Galleon Centre who need the information for their work or an authorised recipient.
- Great care should be taken to establish the identity of any person asking for personal information and to make sure that the person is entitled to receive the information.
- If a staff member is asked by an unauthorised individual to provide details of personal information held by the Galleon Centre the staff member should ask the

individual to put their request in writing and send it to the Deputy General Manager. If the request is in writing the staff member should pass it immediately to their line manager or Deputy General Manager.

- Staff members must not use personal information for any purpose other than their work for the Galleon Centre.
- If a staff member is in doubt about any matter to do with data protection they must refer the matter to their line manager or Deputy General Manager immediately.
- Passwords should not be disclosed and should be changed regularly;
- Staff member or third party personal data should not be left unsecured or unattended, e.g. on public transport;
- Unauthorised use of computer equipment issued by the Galleon Centre is not permitted.
- Staff members must ensure that all confidential information, whether containing staff member or third party personal data or not, is secured when it is not in use or when the staff member is not at work;
- Staff members may use only Galleon Centre equipment to carry out work and must ensure that devices are password protected and locked when not in use. If required, staff members may use personal equipment to carry out work but must ensure that devices are password protected, locked when not in use and must not store any staff member or third party data locally on their device.
- Emails containing staff member or third party personal data must not be sent from a web-based email system;
- As far as possible, staff member or third party personal data contained in emails and attachments should be anonymised before it is sent by email; and
- Documents containing sensitive information should be password protected and, if the document requires to be transmitted, the document and password should be transmitted separately.

Any breach of the above rules will be taken seriously and, depending on the severity of the matter, may constitute gross misconduct which could lead to summary termination of employment.

DECLARATION

I confirm that I have received a copy of this policy and that I have read and understood it.

Name: _____

Signature: _____

Date: _____

STAFF MEMBER DATA

Type of personal data	Sensitive data?	Purpose of processing	Potential transfer to third parties	Lawful basis for processing	Grounds for processing sensitive personal data	Retention period
Contact details	No	Administering the employment contract	HMRC / Professional advisors	Legal obligation / Performance of contract	N/A	6 years post-application
Date of birth	No	Equal opportunities monitoring	Professional advisors	Legal obligation / Performance of contract	N/A	6 years post-application
Gender	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation / Performance of contract	employment purposes / statistics / conduct of legal claims	6 years post-application
Marital status	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation / Legitimate interests	employment purposes / statistics / conduct of legal claims	6 years post-application
Information about race	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation / Legitimate interests	employment purposes / statistics / conduct of legal claims	6 years post-application
Information about ethnicity	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation	employment purposes / statistics / conduct of legal claims	6 years post-application
Information about religious beliefs	Yes	Equal opportunities monitoring	Professional advisors	Legal obligation / Legitimate interests	employment purposes / statistics / conduct of legal claims	6 years post-application
Emergency contact	No	Safety and security	N/A	Legitimate interests	N/A	During employment
NI Number	No	Payroll	HMRC/ Professional advisors	Legal obligation	N/A	6 years post-employment
Salary Information	No	Payroll	HMRC/ Professional advisors	Legal obligation / Performance of contract	N/A	6 years post-employment
Bank Details	No	Payroll	HMRC	Legal obligation / Performance of contract	N/A	6 months post-employment
Tax Details	No	Payroll	HMRC	Legal obligation / Performance of contract	N/A	6 years post-employment
Pension details	No	Payroll / liaising with pension providers	HMRC / Pension Providers	Legal obligation / Performance of contract	N/A	75 years post-employment
Benefits information	No	Providing benefits to staff members	Benefit providers / professional advisors	Legal obligation	N/A	6 years post-employment
Driving license	No	Making recruitment decisions / ascertaining ability to work	N/A	Legal obligation / Performance of contract	N/A	6 years post-application
CV	No	Making recruitment decisions / ascertaining ability to work	N/A	Performance of contract / Legitimate interests	N/A	6 years post-application
Right to work documents	Yes	Checking right to work in the UK	Professional advisors	Legal obligation / Performance of contract	employment purposes / conduct of legal claims	2 years post-application
Sick leave details	No	Managing absence	Professional advisors	Legal obligation / Performance of contract	N/A	6 years post-employment
Performance details	No	Managing performance	Professional advisors	Performance of contract	N/A	6 years post-employment

Qualifications	No	Making recruitment decisions / ascertaining ability to work	Professional advisors	Performance of contract / Legitimate interests	N/A	6 years post- application
Employment history	No	Making recruitment decisions / ascertaining ability to work	N/A	Performance of contract / Legitimate interests	N/A	6 years post- application
Information about disability	Yes	Managing staff / Health and safety requirements / ascertaining fitness to work	Professional advisors	Performance of contract / Legitimate interests	employment purposes / statistics / conduct of legal claims	6 years post- application
Training Records	No	Education, training and development requirements	Professional advisors	Performance of contract / Legitimate interests	N/A	6 years post- employment
Professional memberships	No	Education, training and development requirements	N/A	Legitimate interests	N/A	6 years post- application
Disciplinary and grievance information	No	Staff management	Professional advisors	Performance of contract	N/A	6 years post- employment
CCTV footage	No	Safety and security	Professional advisors	Performance of contract	N/A	6 years post- employment
Information about use of IT systems	No	Ensuring network and data security / staff management	Professional advisors	Performance of contract	N/A	6 years post- employment
Photographs	No	Safety and security	N/A	Legal obligation / Performance of contract	N/A	During employment
Trade union membership	Yes	Deducting trade union fees	Professional advisors	Legitimate interests	employment purposes / conduct of legal claims	6 years post- employment
Health records	Yes	Managing absence / ascertaining fitness to work	Professional advisors	Performance of contract / Legitimate interests	employment purposes / conduct of legal claims	6 years post- application
Genetic information and biometric data	Yes	Managing absence / ascertaining fitness to work	Professional advisors	Performance of contract / Legitimate interests	employment purposes / conduct of legal claims	6 years post- application
Criminal convictions and offences	Yes	Making decisions about recruitment / continued employment	Professional advisors	Legal obligation / Performance of contract	employment purposes / conduct of legal claims	6 years post- application