

# DATA PROTECTION POLICY



# DATA PROTECTION POLICY

## 1. Introduction

- 1.1 This policy applies to all employees of the Royal Air Force Museum and the Royal Air Force Museum Enterprises Ltd (the "Museum").
- 1.2 The Museum holds personal data about job applicants, employees, clients, suppliers and other individuals for a variety of business purposes, including historical research. Some of this data is held in computer systems, but data protection legislation applies to any system where an individual can be identified by name, such as card indexes.
- 1.3 This policy sets out how the Museum seeks to protect personal data and comply with the Data Protection Act 1998, and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work.
- 1.4 In particular, this policy requires staff to ensure that the Museum's Data Protection Officer (currently the Head of Archives) is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.
- 1.5 The Data Protection Officer is responsible for the monitoring and implementation of this policy. If you have any questions about the content of this policy or other comments, you should contact the Data Protection Officer.

## 2. Scope

- 2.1 This policy supplements other Museum policies and procedures, for example, the Computers, Email and Internet Use Policy & Procedures and document retention.
- 2.2 The Museum may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

## 3. Definitions

3. In this policy:

- 3.1 **'Business purposes'** means the purposes for which personal data may be used by the Museum, such as personnel, payroll,

administrative, financial, regulatory, and development purposes, together with collections management and historical research.

- 3.2 **'Personal data'** means information relating to identifiable living individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers, contacts and visitors. This includes expression of opinion about the individual and any indication of someone else's intentions towards the individual.
- 3.3 **'Sensitive personal data'** means personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, sexual life, criminal offences, or related proceedings. Any use of sensitive personal data must be strictly controlled in accordance with this policy.
- 3.4 **'Processing data'** means obtaining, recording, holding or doing anything with it, such as organising, using, altering, retrieving, disclosing or deleting it.

#### 4. General Principles

- 4.1 The Museum's policy is to process personal data in accordance with the applicable data protection laws and the rights of individuals as set out below. All employees have personal responsibility for the practical application of the Museum's Data Protection Policy.
- 4.2 The Museum will observe the following principles in respect of the processing of personal data:
- i. Process personal data fairly and lawfully in line with individuals' rights;
  - ii. Make sure that any personal data processed for a specific purpose is adequate, relevant and not excessive for that purpose;
  - iii. Keep personal data accurate and up to date;
  - iv. Keep personal data for no longer than is necessary;
  - v. Keep personal data secure against loss or misuse;
  - vi. Not to transfer personal data outside the European Economic Area (EEA), which includes the EU countries, Norway, Iceland and Liechtenstein, without adequate protection.

#### 5. Fair and Lawful Processing

- 5.1 Staff should generally not process personal data unless:

- i. The individual whose details are being processed has consented to this;
- ii. The processing is necessary to perform the Museum's legal obligations or to exercise legal rights, or
- iii. The processing is otherwise in the Museum's legitimate interests and does not unduly prejudice the individual's privacy.

5.2 When gathering personal data or establishing new data protection activities, staff should ensure that individuals whose data is being processed receive appropriate data protection notices to inform them how the data will be used. There are limited exceptions to this notice requirement. In any case, of uncertainty as to whether a notification should be given, staff should contact the Data Protection Officer.

5.3 It will normally be necessary to have an individual's explicit consent to process 'sensitive personal data', unless exceptional circumstances apply or the processing is necessary to comply with a legal requirement. The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the Data Protection Officer for more information on obtaining consent to process sensitive personal data.

## **6. Accuracy, Adequacy, Relevance and Proportionality**

6.1 Staff must make sure that data processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

6.2 Individuals may ask the Museum to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the Data Protection Officer.

6.3 Staff must ensure that personal data held by the Museum relating to them is accurate and updated as required. If personal details or circumstances change, staff should inform the Personnel Department so the Museum's records can be updated.

## **7. Security**

- 7.1 Staff must keep personal data secure against loss or misuse. Where the Museum uses external organisations to process personal data on its behalf additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. Staff should consult the Data Protection Officer to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement.

## **8. Data Retention**

- 8.1 Personal data should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data were obtained.

## **9. International Transfer**

- 9.1 Staff must not transfer personal data internationally and/or outside the EEA (as defined in 4.2 above) without first consulting the Data Protection Officer. There are restrictions on international transfers of personal data to other countries because of the need to ensure that adequate safeguards are in place to protect the personal data. Staff unsure of what arrangements have been, or need to be, put in place to address this requirement should contact the Data Protection Officer.

## **10. Rights of Individuals**

- 10.1 Individuals are entitled (subject to certain exceptions) to request access to information held about them. All such requests should be referred immediately to the Data Protection Officer. This is particularly important because the Museum must respond to a valid request within the legally prescribed time limit, normally 40 days.
- 10.2 Any member of staff who would like to correct or request information that the Museum holds relating to them should contact the Data Protection Officer who will liaise with the appropriate department(s). The Museum will charge a fee of £10.00 for providing the requested personal data, as permitted by law. It should be noted that there are certain restrictions on the information to which individuals are entitled under applicable law.

10.3 Staff must not send direct marketing material to someone electronically (e.g. by email) unless there is an existing business relationship with them in relation to the services being marketed. Staff must abide by any request from an individual not to use their personal data for direct marketing purposes and should notify the Head of Marketing about any such request and advice on direct marketing before starting any new direct marketing activity.

## 11. Reporting Breaches

11. Staff have an obligation to report actual or potential data protection compliance failures to the Data Protection Officer. This allows the Museum to:

- i. Investigate the failure and take remedial steps if necessary; and
- ii. Make any applicable notifications.

## 12. Consequences of Failing to Comply

12.1 The Museum takes compliance with this policy very seriously.

12.2 Failure to comply puts both staff and the Museum at risk.

12.3 The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

12.4 Staff with any questions or concerns about anything in this policy should not hesitate to discuss these with either line management or the Data Protection Officer.

### Policy Monitoring:

Responsibility for the review and development of this policy lies with the Data Protection Officer. Day to day operation, the implementation and monitoring of this policy is the responsibility of Line Managers and staff who should ensure that it is followed.