

# General Data Protection Regulations

## Data Protection Policy

The Visitor Information Centre (VIC) is committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of data in order to carry on our work.

The Data Protection Act 1998 (DPA) and the General Data Protection Regulations (GDPR) govern the use of information about people known as **Personal Data** which shall be collected and handled securely. **Personal Data** may be held on laptops, computers and mobile devices or in a manual file and includes e-mails, minutes of meetings and photographs.

The Secretary of the VIC is the Data Controller for the information held. The VIC is personally responsible for holding and using personal information in accordance with the DPA and the GDPR.

The VIC shall comply with this policy.

## Data Protection Arrangements

### 1 INTRODUCTION

1.1 The VIC regards the lawful and correct treatment of **Personal Data** as very important to successful working and to maintain the confidence of those with whom we deal. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

1.2 The following are definitions of the terms used:

- (i) **Data Controller** – the Secretary is the person who decides what personal data the VIC will hold, who will hold it and how it will be held or used.
- (ii) **Act** means DPA 1998 and the GDPR – the legislation that requires responsible behaviour by those using personal information.
- (iii) **Data Subject** means the individual whose personal information is being held or processed by VIC for the purposes of managing bookings and lettings.
- (iv) **Processing** means collecting, amending, handling, storing or disclosing personal information.
- (v) **Personal Data** means information about living individuals that enables them to be identified and shall include:
  - Online identifiers (emails)
  - Trustee, Committee and employee information

- Databases holding contact information (bookings, mailings)
- CCTV footage
- Financial information
- Publicity information
- Fundraising purposes (individual donors)

## **2 RESPONSIBILITIES**

- 2.1 The VIC will take into account the Act, ensure they are properly implemented and will specifically through this procedure, and apply strict controls.
- 2.2 The Secretary, as Data Controller, shall be responsible for ensuring that the procedure is implemented and will have overall responsibility for:
- (i) Ensuring the VIC implement its procedure
  - (ii) Dealing promptly and courteously with all enquires
  - (ii) Managing any breach of the DPA in compliance with this procedure

## **3. COLLECTING PERSONAL DATA**

- 3.1 We will let people know why we are collecting their **Personal Data** for, its activities and its finances
- 3.2 It is the responsibility of the VIC to ensure that data is only used for these purposes.
- 3.3 Access to Personal Data shall be limited to the VIC.
- 3.4 The following statement shall be visible on the VIC website and its procedures where applicable:

This message may not be copied, disclosed or used by anyone other than the intended recipient. If you are not the intended recipient please delete this email. The VIC is a Limited Company and has certain powers and obligations. Most personal data will be processed for compliance with a legal obligation which includes the discharge of the VIC's statutory functions and power where the use of personal data requires an individual's consent, the VIC will obtain consent to that use. Further information regarding how the VIC processes personal data is available below (Word document attached)

## **4 USE AND STORAGE OF PERSONAL DATA**

- 4.1 It shall be processed fairly and lawfully and in compliance with VIC's established procedures

- 4.2 It shall be obtained only for the reasons stated in the procedures and shall not be processed in any manner incompatible with those purposes
- 4.3 It shall be adequate, relevant and not excessive in relation to those purposes
- 4.4 It shall be accurate and, where necessary, kept up to date
- 4.5 It shall not be kept for longer than necessary.
- 4.6 It shall be processed in accordance with the rights of data subjects under the Act
- 4.7 It shall be kept secure by those appointed with responsibilities who shall take appropriate technical or other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of **Personal Data**.
  - (i) All laptops and portable devices that hold Personal Data shall be protected by password
  - (ii) Personal data shall not be stored on memory sticks
  - (iii) The VIC shall operate a “clear desk policy”
  - (iv) Hard copy records kept in the safe by VIC shall be maintained securely
  - (v) Emails shall be saved in the appropriate folders and when printed, stored securely if required.
  - (vi) No personal information shall be given out over the telephone unless the person’s identity is confirmed and the request is valid.
  - (vii) Completed pages from the Accident Book shall be removed and when appropriate action taken and stored securely

## 5 **CORRECTING PERSONAL DATA**

- 5.1 Individuals have a right to make a Subject Access Request (SAR) to find out whether the VIC holds their **Personal Data**, where it is, what it is used for and to have the data corrected if it is wrong. They also have the right to prevent its use if it is causing them damage or distress or to stop marketing information being set to them.
- 5.2 All SARs shall be dealt with within 30 days. Steps shall first be taken to confirm the identity of the individual making the request before providing information. This will require:
  - (i) Photo identity (passport etc)
  - (ii) Confirmation of address (utility bill, etc)Failure to produce this evidence shall nullify the SAR.

## 6 BREACHING THE DPA

- 6.1 We are required to report certain types of **Personal Data** breach to the Information Commissioners Office (ICO) and in some cases to the individuals affected.
- 6.2 A **Personal Data** breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. The ICO shall be notified where it is likely to result in injury to an individual. The report shall be made within 72 hours of becoming aware that an incident is reportable. Where there is doubt as to whether the breach is reportable, clarification shall be obtained from the ICO helpline on 0303 123 1113.
- 6.3 All breach of the DPA, reportable or not, shall be investigated to prevent recurrence.