

# Data Protection Policy

This policy applies to all trustees, committee members and volunteers of Fair Game UK.

## 1. Introduction

In order for Fair Game UK to deliver its work and objectives, to operate effectively as a charity, and to meet its obligations to its customers, we process personal data relating to present, past and potential stakeholders.

## 2. Definition of “Personal Data”

The GDPR applies to “personal data”, meaning any information relating to an identifiable person who can be directly or indirectly identified by that data. For example, this could include name, address, e-mail address, date of birth, bank details, and so on. In order to reflect technological changes, GDPR also defines personal data to include elements such as location data or other online identifiers such as IP address.

“Special Category” (SC) data is personal data which the GDPR identifies as more sensitive, and so requires further protection. This SC data can include identifiers such as race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.

## 3. Scope

This policy applies to all those individuals and organisations that process personal data on behalf of Fair Game UK, including but not limited to:

- Volunteers, consultants, contractors and temporary staff
- Trustees, Committee Members and any other advisers
- Suppliers and partners of Fair Game UK
- Other third parties associated with Fair Game UK

## 4. Policy

This policy helps to show the commitment of Fair Game UK to complying with all relevant data protection legislation. We support ensuring that personal data is handled appropriately, securely and sensitively, as well as ensuring that all data is accurate and only held for the period for which it is required.

Our people take action that significantly reduces the likelihood of an information security breach and its wider effects including causing harm or distress to data subjects, reputational damage, potential fines and any further sanctions from the Information Commissioner.

FGUK is committed to protecting the rights and freedoms of individuals in accordance with the provisions of all relevant data protection legislation.

FGUK ensures that all personal data is:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes

- Adequate, relevant and limited to what is necessary in relation to the purposes for which is held
- Accurate and up to date, ensuring that inaccurate data is rectified without delay
- Kept in line with our Retention Guidance to ensure that personal data is only kept as long as it is required for the purpose it is held
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

## 5. Data Protection Officer

Fair Game UK is a data controller and a data processor. FGUK will ensure that it meets all requirements of the Data Protection Act, and any other data protection regulations. A data protection officer will be appointed.

## 6. Holding Personal Data

Ensuring personal data is collected and held in an appropriate manner is key to the successful operation of Fair Game UK, including upholding trust and our reputation with our partners, stakeholders and customers. In order to achieve this, FGUK will:

- Undertake a Data Protection Impact Assessment for new programmes of work (including new software) that involves collecting, sharing or processing personal data, where this is likely to result in potential risks to the rights and freedoms of data subjects.
- Identify a lawful basis in data protection legislation for collecting and sharing personal data.
- Collect, process and share the minimum amount of personal data required to achieve the objective(s).
- Use anonymised data where the identification of data subjects is not required for the purpose of processing.
- Provide data subjects with privacy notices and clear guidance on how to exercise their rights via Fair Game UK website.
- Record all decisions to share personal data with external partners.
- Ensure that a data sharing arrangement is in place where personal data is shared with external partners or there is a large scale transfer of personal data.
- Ensure that data is not transferred to a country outside the UK or the European Economic Area, unless that country has an Adequate level of protection for personal data as defined in law.

## 7. Legal reasons for processing Personal Data

Personal data can only be lawfully processed if the processing is deemed necessary under one of the

following circumstances (Lawful Bases as set out by the Information Commissioner's Office):

**(a) Consent:** the individual has given clear consent for us to process their personal data for a specific purpose.

**(b) Contract:** the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

**(c) Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).

**(d) Vital interests:** the processing is necessary to protect someone's life.

**(e) Public task:** the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

**(f) Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

All personal data held by Fair Game UK must fall under one of these lawful bases and that lawful basis must be recorded for processing to be carried out lawfully. This will be recorded by the DPO/COO. FGUK may record special category information, and should this be required, additional safeguards are needed. Before holding such information, FGUK must formally record why this is necessary, what the basis is, and what steps are being taken to protect it.

### **7.1 Children's data**

Children aged 12 and over have the right to be informed and manage their own data. The same lawful bases as listed above also apply to children. (For children under 12, parental consent to process is required). The rights and freedoms of children are the same as for adults, including the requests covered later in this document.

## **8. Obligations and Responsibilities of our people**

All of our people are obliged to:

- Ensure that any information they provide to FGUK about themselves is accurate and up-to-date, and inform their line manager of any changes to their information, for example their address.
- Provide information in response to Data Protection audits and data breach investigations
- In the event of a subject access request, provide all relevant information to the DPO
- Undertake training on Data Protection and Information Security

Senior management are responsible for ensuring that all volunteers are aware of their responsibilities in relation to data management. Data Protection training will be mandatory for all staff.

All our people are responsible for ensuring that:

- Any personal data they hold is kept securely and in line with relevant internal policies;
- Personal data is not disclosed accidentally or otherwise to any third party without authorisation.

Our people should note that unauthorised disclosures will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

All our people should ensure that personal data is:

- when kept in hardcopy – including at home – is kept securely, such as in a locked drawer.

- not visible to anyone not authorised to see it, either on desks or on computer screens, including by family members, other members of their household, or by others in shared working facilities.
- stored on private network folders and if appropriate, password protected.
- not sent via e-mail without password protection or encryption, if it contains special category personal data, banking information, or data about children.
- not saved directly onto laptops, flash drives, or other portable media

People should be aware that any information linked to an individual can be requested by that individual. Therefore, any remarks and annotations related to individuals should be appropriate, justified and relevant.

## **9. Subject Rights and Subject Access Requests (SARS)**

The Data Protection Act/GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Everyone has the right of access to personal data that is being kept about them. Anyone wishing to make a request should do so in writing via [governance@fairgameuk.org](mailto:governance@fairgameuk.org) with details of the information requested, and proof of identification.

Anyone receiving a request should forward this to the DPO who will deal with the request. FGUK will reply within one calendar month.

## **10. Security and Retention of Data**

All records (including electronic, printed and handwritten) must be held securely to prevent unauthorised or unlawful processing or disclosure of data. Appropriate measures should be taken to minimise the possibility of accidental loss, destruction or damage to personal data. Our people must not store Foundation data on personal equipment, mobile phones or other personal storage equipment. Access to data must be limited to legitimate users only. Access to electronic records will be controlled through password protection and varying levels of access. Records should be kept only for as long as is necessary and then destroyed in line with the retention policy.

## **11. Breach Reporting**

A personal data breach is defined as: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data”.

FGUK is responsible for ensuring appropriate and proportionate security for the personal data that we hold. FGUK makes every effort to avoid personal data breaches, however, it is possible that data breaches will occur. Examples of personal data breaches include:

- Loss or theft of data or equipment
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

If a data protection breach occurs, FGUK is required in most circumstances to report this as soon as possible to the Information Commissioner's Office, and not later than 72 hours after becoming aware of it. All breaches of this policy and data protection legislation must be reported immediately to the DPO/COO, including out of hours, and staff must take the action requested of them – such as complying with an investigation, contacting IT for support to secure an account, or informing others of virus or phishing attacks. Failing to do so may result in disciplinary action. A breach by a third party may result in a termination of contract.

## **12. Impact of non-compliance**

All volunteers are required to comply with this Data Protection Policy, the supporting guidance and the requirements specified in the DPA/GDPR. Anyone who is found to have made an unauthorised disclosure of personal information or breached the terms of this Policy will be in breach of the Code of Conduct. People including our volunteers may also incur criminal liability if they knowingly or recklessly obtain and/or disclose personal information for their own purposes, which are outside the legitimate purposes of FGUK. FGUK could be fined for non-compliance with the GDPR.

## **Contacts**

FGUK's named Data Protection Officer is Elizabeth Anderson. If you have any queries, or are approached about any requests, a breach or any other data protection matter, please contact her.

September 2022