**Data Protection and Records Management Policy**

**Revised June 2021**

**DATA PROTECTION AND RECORDS MANAGEMENT POLICY**

**Contents**

1 Introduction 4

1.1 StreetGames’ commitment to data protection 4

2 Definitions 4

3 Policy scope 6

3.1 Responsibility for the policy 6

3.2 Policy aim 6

3.3 Policy application 6

4 Data protection principles 6

4.1 StreetGames’ data protection policy is set within the context of the Data Protection Principles set out within the GDPR: 6

5 Responsibilities under the policy 7

5.1 Responsibilities of StreetGames 7

5.2 Responsibilities of all StreetGames employees 7

5.3 Responsibilities of the Data Protection Officer (DPO) 7

5.4 Responsibilities of the IT Manager 8

5.5 Responsibilities of the Director of Fundraising and Communications 8

5.6 Responsibilities of other management leads 8

6 Managing risk 9

6.1 Privacy by design and default 9

7 Data collection 9

7.1 Documentation 9

7.2 Valid reasons for processing data: 9

7.3 Transparency 10

8 Processing of data 10

8.1 Fair and lawful processing 10

8.2 Processing data in accordance with the individual's rights 11

8.3 Sensitive personal data 11

8.4 Conditions for processing 11

8.5 Accuracy and relevance 11

8.6 Data security 12

8.7 Storing data securely 12

8.8 Data retention 12

8.9 Right to be forgotten 13

8.10 Transferring data internationally 13

8.11 Subject access requests 13

9 Training 14

9.1 Staff training 14

9.2 Training content and materials 14

10 Reporting breaches 14

11 Failing to comply 14

11.1 Consequences 14

12 Appendix 1: StreetGames Data Breach Procedure 15

12.1 Aim of the procedure 15

12.2 Why we respond to incidents 15

12.3 What is a data breach? 15

12.4 How do we prevent breaches? 15

12.5 Responsibilities 16

# Introduction

## StreetGames’ commitment to data protection

#### StreetGames is committed to conducting its business in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

#### We hold personal data about our employees, participants, volunteers, funders, suppliers, beneficiaries and other individuals for a variety of business purposes.

### Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data.

#### An organisation that handles personal data and makes decisions about its use is known as a Data Controller. StreetGames, as a data controller, is responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose StreetGames to complaints, regulatory action, fines and/or reputational damage.

#### StreetGames is fully committed to ensuring continued and effective implementation of this policy, and expects all employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

### This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

# Definitions

|  |
| --- |
| **Definitions of the key terms used in this policy** |

|  |  |
| --- | --- |
| Anonymisation | Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person. |
| Business purposes | The purposes for which StreetGames may use personal data, including: personnel, administrative, financial, regulatory, payroll and business development purposes.  Business purposes include the following:   * Compliance with our legal, regulatory and corporate governance obligations and good practice. * Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests. * Ensuring business policies are adhered to (such as policies covering email and internet use). * Operational reasons, such as recording participants’ data, quality control, ensuring the confidentiality of commercially sensitive information. * Investigating complaints. * Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments. * Monitoring staff conduct, disciplinary matters. * Marketing our business. * Improving services. |
| Data controller | An individual or organisation who determines the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. StreetGames is the data controller of all personal data used in its business. |
| Data processor | Any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on StreetGames’ behalf. |
| Data protection | The process of safeguarding personal data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction. |
| Data Protection Office (DPO) | * DPOs assist in monitoring internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner’s Office (ICO).  StreetGames is not required by law to appoint a DPO and has currently chosen not to do so. Nevertheless, we take our responsibilities with respect to data protection seriously. As such, the Director of Finance and Resources leads on ensuring that StreetGames’ activities comply with the legislation. All references to the DPO within this document should be read as referring to the Director of Finance and Resources. |
| Data subject | All living individuals about whom StreetGames holds personal data. The Data Protection Act 2018 (The Act) does not count as a data subject an individual who has died or who cannot be identified or distinguished from others. |
| Personal data | Data relating to a living individual who can be identified from that data (or from that data and other information in possession of StreetGames). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can even include a simple e-mail address. It is important that the information has the data subject as its focus and affects the individual's privacy in some way. Mere mention of someone's name in a document does not constitute personal data, but personal details such as someone's contact details or salary would still fall within the scope of the Act. |
| Privacy Impact Assessment (PIA) | Also known as Data protection impact assessments (DPIAs). These are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals’ expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur. |
| Processing | Any activity that involves use of data. This 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 transferring personal data to third parties. |
| Profiling | Any form of automated processing of personal data where personal data is used to evaluate specific or general characteristics relating to an identifiable natural person. In particular to analyse or predict certain aspects concerning that natural person’s performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement. |
| Pseudonymisation | Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a “key” that allows the data to be re-identified. |
| Sensitive personal data (special categories of data) | Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), sexual orientation, physical or mental health or condition, criminal offences, or related proceedings. Any use of sensitive personal data should be strictly controlled in accordance with this policy. |

# Policy scope

## Responsibility for the policy

#### The Data Protection Officer has overall responsibility for the day-to-day implementation of this policy.

## Policy aim

#### The aim of this policy is to set standards for processing data and responding to requests for information as required by relevant legislation such as the Data Protection Act 2018, the Freedom of Information Act, and the Environmental Information Regulations.

## Policy application

#### This policy sets out the expected behaviours of StreetGames employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to a StreetGames contact (i.e. the data subject).

#### This policy applies to information about individuals as well as StreetGames as an organisation. It governs requests made in any form for access to data recorded in any medium by any person including participants, funders, trustees, and employees.

#### This policy applies to all StreetGames activities where a data subject’s personal data is processed.

#### This policy supplements StreetGames’ other policies, including the IT Policy, Safeguarding Policy, Fundraising Policy and the Staff Handbook. We may supplement or amend this policy by additional policies and guidelines from time to time.

# Data protection principles

## StreetGames’ data protection policy is set within the context of the Data Protection Principles set out within the Act:

#### *Principle 1: Lawfulness, Fairness and Transparency*. Personal data shall be processed lawfully, fairly and in a transparent manner.

#### *Principle 2: Purpose Limitation*. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

#### *Principle 3: Data Minimisation*. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

#### *Principle 4: Accuracy*. Personal data shall be accurate and, where necessary, kept up to date.

#### *Principle 5: Storage Limitation*. Personal data shall be kept in a form which permits identification of data subjects for not longer than is necessary for the purposes for which the personal data are processed.

#### *Principle 6: Integrity & Confidentiality*. Personal data shall be processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

# Responsibilities under the policy

## Responsibilities of StreetGames

#### StreetGames is required to comply, and to clearly demonstrate howit complies, with the data protection principles.

## Responsibilities of all StreetGames employees

#### Understanding and adhering to this policy.

#### Taking reasonable steps to ensure that personal data StreetGames holds about them is accurate and updated as required. For example, if their personal circumstances change, please inform the relevant individual so that they can update your records.

## Responsibilities of the Data Protection Officer (DPO)

#### Keeping the board updated about data protection responsibilities, risks and issues.

#### Reviewing and monitoring all data protection procedures and policies on a regular basis.

### Arranging data protection training and advice for all staff members and those included in this policy.

### Answering questions on data protection from staff, board members and other stakeholders.

### Ensuring responses are made to individuals such as participants, funders, and employees who wish to know which data is being held on them by StreetGames.

### Ensuring establishment of procedures for obtaining compliance with this policy by any third party who: provides personal data to StreetGames, receives personal data from StreetGames, or has access to personal data collected or processed by StreetGames.

### Detailing what data is held across the organisation, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

## Responsibilities of the IT Manager

### Ensuring all systems, services, software and equipment meet acceptable security standards.

### Checking and scanning security hardware and software regularly to ensure it is functioning properly.

### Researching third party services, such as cloud services the company is considering using to store or process data.

## Responsibilities of the Director of Fundraising and Communications

### Approving data protection statements attached to emails and other marketing copy.

### Addressing data protection queries from target audiences or media outlets.

### Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company’s Data Protection Policy.

### Ensuring media used by StreetGames adheres to data protection laws and this policy.

## Responsibilities of other management leads

### Carrying out regular data audits to manage and mitigate risks and to inform the data register.

### Checking and approving with third parties that handle StreetGames’ data, including any contracts or agreements regarding data processing.

### Keeping the DPO informed of any issues that impact on his/ her responsibilities.

# Managing risk

## Privacy by design and default

### Privacy by design is an approach that promotes privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments (PIA).

### A PIA should be conducted when StreetGames seeks to introduce new technologies, and when processing is likely to result in a high risk to the rights and freedoms of individuals. PIA’s should seek to follow the Information Commissioners Office’s (ICO) [Code of Practice](https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf).

### Processing that is likely to result in a high risk includes (but is not limited to):

* Systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
* Large scale processing of special categories of data or personal data in relation to criminal convictions or offences.

### When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

# Data collection

## Documentation

#### StreetGames will document the justification for the processing of personal and sensitive data and will ensure any biometric and genetic data is considered sensitive.

## Valid reasons for processing data:

#### The individual whom the data is about has consented to the processing.

#### StreetGames believes that by empowering individuals to decide how their personal data is used their consent is properly informed. It also fosters trust in the organisation and allows us to use our data more effectively.

#### The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

#### Consent must be a freely given, specific, informed and unambiguous indication of the individual’s wishes.

#### There must be some form of clear affirmative action – or in other words, a positive opt-in. Consent cannot be inferred from silence, pre-ticked boxes or inactivity.

#### Consent must be separate from other terms and conditions, and there must be clear and simple ways for people to withdraw consent.

#### Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data.

#### There are some cases in which consent is not relevant, for example if individuals are required by law to provide their personal details. Giving people control and choice over how their personal data will be processed will not always be applicable in other situations, for example in an employer/employee relationship. StreetGames will ensure fairness and transparency in communicating these instances.

#### The processing is necessary in relation to a contract which the individual has entered into or because the individual has asked for something to be done so they can enter into a contract, e.g. an employment contract or a contract for the provision of services.

#### The processing is necessary because of a legal obligation that applies to StreetGames.

#### The processing is necessary to protect the individual’s ‘vital interests’.

#### The processing is necessary for administering justice, or for exercising statutory, governmental or other public functions.

#### The processing is in accordance with the ‘legitimate interests’ condition. In considering what might constitute a legitimate interest we should bear in mind that:

#### Processing should not harm the interests of a data subject.

#### It is not applicable in situations where data subjects would not reasonably expect further processing.

#### The data subject must be informed about the purpose of collection and about their right to object.

#### In practice, StreetGames is most likely to rely on the provisions within sections 7.2.2, 7.2.3 and 7.2.6 in order to process personal data.

## Transparency

#### StreetGames will be transparent and provide accessible information via a privacy notice to individuals about why we are processing their personal data and how we will use it.

# Processing of data

## Fair and lawful processing

### StreetGames must process personal data fairly and lawfully in accordance with individuals’ rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening or there are other legitimate reasons for doing so in line with the principles set out in s7 above.

### The processing of data must be necessary to deliver our services, in our legitimate interests and not unduly prejudice the individual's privacy.

## Processing data in accordance with the individual's rights

### Any request from an individual not to use their personal data for direct marketing purposes should be abided.

### Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

### Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

## Sensitive personal data

### In most cases where StreetGames processes special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

## Conditions for processing

### StreetGames will ensure any use of personal data is justified, using at least one of the conditions for processing set out in s7 above and this will be specifically documented.

### Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means StreetGames must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

### Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means that StreetGames must not store any personal data beyond what is strictly required.

### All staff responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

## Accuracy and relevance

### StreetGames will ensure that any personal data processed is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained.

### StreetGames will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

### Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the data owner.

## Data security

### Personal data must be kept secure against loss or misuse. Where other organisations process personal data, as a service on StreetGames’ behalf, there might be additional specific data security arrangements to be implemented in contracts with those third party organisations. Advice should be sought from the DPO.

## Storing data securely

### In cases when data is stored on printed-paper, it should be kept in a secure place where unauthorised personnel cannot access it.

### Printed data should be shredded when it is no longer needed.

### Data stored electronically should be stored in accordance with the StreetGames IT Policy. Ideally data should be stored on the StreetGames Teams Site (SharePoint) or One Drive. Where this is not possible the data should be encrypted and encrypted devices are available from the IT manager to enable this.

### Employees whose roles require them to travel frequently or work in public places on StreetGames business should seek to ensure they do not have sensitive data visible on their screen. If this is unavoidable, laptops should have privacy screens installed.

### Data stored on CDs, memory sticks or external hard drives, even when encrypted, must be locked away securely when they are not being used.

### The IT Manager must approve any alternative cloud storage used to store data.

### Servers containing personal data must be kept in a secure location.

### Data should be regularly backed up in line with the company’s backup procedures.

### All servers containing sensitive data must be approved and protected by security software and a strong firewall.

## Data retention

### Personal data must not be retained for longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained.

### Retention periods, and the reasons for them, should be decided at creation and documented for all data.

### Staff should carry out regular reviews of data and records held to assess the need for their continued retention and the risk of a potential data breach. In cases of uncertainty, staff should refer to the DPO for guidance.

### Personal data shall be kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means StreetGames must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

## Right to be forgotten

### A data subject may request that any information held on them is deleted or removed.

### Any third parties who process or use that data must also comply with a request for information to be deleted or removed.

### An erasure request can only be refused if an exemption applies.

## Transferring data internationally

### There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the DPO.

### Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

## Subject access requests

### Please note that under the Data Protection Act 2018 individuals are entitled, subject to certain exceptions, to request access to information held about them.

### If you receive a subject access request, you should refer that request immediately to the DPO who will liaise with the relevant data owner to ensure this is logged and dealt with within the appropriate timescales.

### There are restrictions on the information to which a data subject is entitled to access under applicable law.

### Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

# Training

## Staff training

### All staff will receive training on this policy. New employees will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

## Training content and materials

### Training will cover the law relating to data protection and StreetGames’ data protection and related policies and procedures.

### Completion of training is compulsory.

# Reporting breaches

### All members of staff have an obligation to report actual or potential data protection compliance failures. This allows StreetGames to:

* Investigate the failure and take remedial steps if necessary.
* Maintain a register of compliance failures.
* Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures.

### Compliance failures should be reported in the first instance to the DPO.

# Failing to comply

## Consequences

### StreetGames takes compliance with this policyvery seriously. Failure to comply puts third parties, employees and StreetGames at risk.

### The importance of this policy means that failure to comply by an employee with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.

### The importance of this policy means that failure to comply by a third party with any requirement may lead to business sanctions.

### If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

# Appendix 1: StreetGames Data Breach Procedure

## Aim of the procedure

### The Data Breach Procedure provides assurances that appropriate measures are in place to handle security incidents – in isolation and across the organisation as a whole.

## Why we respond to incidents

### The purpose of an incident response is to ensure that:

* Data breach events are detected, reported, categorised and monitored consistently
* Incidents are assessed and responded to appropriately
* Action is taken to reduce the impact of disclosure
* Mitigation improvements are made is put in place to prevent recurrence
* Serious breaches can be reported to the Information Commissioner
* Lessons learnt are communicated to the organisation as appropriate and can work to prevent future incidents.

### Not all data protection breaches will result in formal action. Some will be false alarms or “near miss” events that do not cause immediate harm to individuals or the organisation. These should still be logged, as analysis of these will allow lessons to be learnt and facilitate continual improvement.

## What is a data breach?

### A Data Protection breach is the result of an event or series of events where personally identifiable information is exposed to unauthorised or inappropriate processing that results in its security being compromised. The extent of damage or potential damage caused will be determined by the volume, sensitivity and exposure of the information.

## How do we prevent breaches?

### Following the policies and procedures that StreetGames has set out will minimise the risk of a data breach.

### Learning from incidents will improve StreetGames’ policies and procedures with recommendations being made at local and organisational level.

### Local recommendations apply purely to the region or department(s) affected by the incident and will usually reflect measures that need to be taken to restrict the chances of the same type of incident occurring.

### Organisational recommendations will follow those incidents caused by factors that are not unique to one department or region but can be found right across the organisation. Issues such as training, information handling and physical security affect all departments and it is essential that StreetGames identifies such risks and puts in place measures to prevent the incident occurring elsewhere.

## Responsibilities

### When an incident occurs (or is likely to occur) where the security of personal data is compromised this should immediately be reported to the relevant data controller and the DPO.

### All incidents will be logged centrally by the DPO.

### The DPO and the data controller will assess what further action is required and who should be included in any assessment. They may decide that it is appropriate to carry out a further and more detailed investigation.

### The aim of an investigation is to identify what actions, if any, need to be taken to prevent a recurrence and to determine if the ICO needs to be notified. All breaches will be reported to the Board.

### It is important that StreetGames fosters a culture that encourages identification of breaches to ensure learning and insights can be gathered to improve processes. Learning and recommendations might be made at an organisational or local level and learning will be shared with staff, the Executive team and the Board as appropriate.