Data Protection Policy

Charity Number SCO 23344

Company Number 379003

1 Overview

1.1 Play Alloa takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

1.2 The Company has separate policies and privacy notices in place in respect of job applicants, customers, suppliers and other categories of data subject. A copy of these can be obtained from the Play Alloa Office/Website.

1.3 The Company has additional measures in place to protect the security of your data in accordance with our Confidentiality Policy, Secure Handling of PVG Policy, and Social Media Policy etc. A copy of these can be obtained from the Play Alloa Office/Website.

1.4 The company will hold data in accordance with this Policy. We will only hold data for as long as necessary for the purposes for which we collected it.

1.5 Play Alloa is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

1.6 This policy explains how Play Alloa will hold and process your information. It explains your rights as a data subject.

2 Data Protection Principles

2.1 Play Alloa will process personal data in accordance with the six '**Data Protection Principles**.' It will:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

3 Your personal data – what is it?

How we define personal data

3.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into Play Alloa's possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data. The processing of personal data is governed by [the General Data Protection Regulation 2016/679 (the "GDPR")

3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

3.3 This personal data might be provided to us by an individual, or someone else, or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be provided during registration for services. It could be created by your manager or other colleagues.

3.4 We will collect **personal data** as follows:

3.4.1 We will collect/use the following types of personal data about staff:

- recruitment information such as application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- contact details and date of birth;
- the contact details for emergency contacts;
- information about contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- bank details and information in relation to tax status including national insurance number;
- identification documents including passport and driving licence and information in relation to immigration status and right to work for us;
- information relating to disciplinary or grievance investigations and proceedings (whether or not an individual is the main subject of those proceedings);
- information relating to performance and behaviour at work;
- training records;

- images (whether captured on CCTV, by photograph or video);
- PVG registration number
- Any other category of personal data which we may notify an individual of from time to time.

3.4.2 We will collect/use the following types of personal data about volunteers:

- recruitment information such as application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- contact details and date of birth;
- the contact details for emergency contacts;
- identification documents including passport and driving licence and information in relation to immigration status and right to work for us;
- information relating to disciplinary or grievance investigations and proceedings (whether or not and individual is the main subject of those proceedings);
- information relating to performance and behaviour at Play Alloa;
- training records;
- images (whether captured on CCTV, by photograph or video);
- PVG registration number
- Any other category of personal data which we may notify an individual of from time to time.

3.4.3 We will collect/use the following types of personal data about Service Users/Parent/Carers:

- Service User name, address, date of birth;
- Information relating to their conditions and medical information;
- which sessions they are assigned to;
- parent/carer contact numbers and email address;
- Involvement with other agencies;
- Management of Service User: e.g. general behaviour, supervision needs, mobility/travel, speech and communication, toileting, feeding, dressing, play interests;
- Photographs – if prior consent has been given on registration forms
- All information and permissions on Service Users is updated every 6 months as per Care Inspectorate recommendations

4 How we define processing

4.1 **'Processing'** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;

- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- Restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

5 How will we process your personal data - What is the legal basis for processing your personal data?

5.1 Play Alloa will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

5.2 These fall under either article 6 or article 9 – dealt with separately below.

Play Alloa has several legal bases for processing personal data: Explicit Consent, Legal Obligation, Vital Interest, Not-for-Profit Organisation, Medical Purposes, and Equality of Opportunity.

Data Protection Act Article 6: Processing

- Consent of the data subject;
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation;
- Processing is necessary to protect the vital interests of a data subject or another person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
- Processing is necessary for the legitimate interests of the data controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Data Protection Act Article 9: Processing

- Explicit consent of the data subject
- Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement;
- Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent;
- Processing is carried out by a not-for-profit body and the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes); and there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject;

- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest on the basis of EU or Member State law;
- Processing is necessary for reasons of preventative or occupational medicine, for assessing the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional;
- Processing is necessary for the reasons of public interest in the area of public health;
- Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

5.3 We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

6 Sharing your personal data

Your personal data will be treated as strictly confidential, and will be shared only within Play Alloa. We will only share your data with third parties outside of the organisation with your consent, unless it relates to a child/vulnerable adult protection issue.

7 How long do we keep your personal data?

We keep your personal data for no longer than reasonably necessary and we only retain your data for the following purposes and use the following criteria to determine how long to retain your personal data;

a. Staff: Information on staff members will be kept for 1 year, after the end of their employment with Play Alloa, for the purpose of being able to provide a reference. Subsequent to the 1 year time period we will remove their information other than their name, sessions worked, start date and end date

b. Volunteers: Information on volunteers will be kept for 1 year, after the end of their volunteering time with Play Alloa, for the purpose of being able to provide a reference. Subsequent to the 1 year time period we will remove

their information other than their name, sessions volunteered at, start date and end date

c. Service Users/Parents/Carers: When a Service User hasn't attended any of our sessions for a period of 3 months, we will make contact to ask a Service User's Parent/Carer if they wish their information to be kept on the system should they choose to return. At this point, if they do not reply or do not wish to remain on the system, we will remove their data other than name, condition, sessions attended, start date and end date for funding reporting purposes.

8 Your rights and your personal data

Unless subject to an exemption [under the GDPR], you have the following rights with respect to your personal data: -

- You have the right to information about what personal data we process, how and on what basis as set out in this policy.

- **The right to request a copy of your personal data** which Play Alloa holds about you by way of a subject access request;
- **The right to request that Play Alloa corrects any personal data** if it is found to be inaccurate or out of date. To do you should contact the Play Alloa Office;
- **The right to be forgotten** where it is no longer necessary for Play Alloa to retain such data or where we were not entitled under the law to process it. To do so you should contact the Play Alloa Office;
- The right to withdraw your consent to the processing at any time, however if you choose to withdraw consent we may not be able to provide our service to you;
- The right to request that Play Alloa provides the data subject with his/her personal data and where possible, to transmit that data directly to another data controller, (known as **the right to data portability**)
- You have **the right to object** to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
- **The right to request a restriction is placed on further processing**, where there is a dispute in relation to the accuracy or processing of your personal data,; While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Play Alloa Office.
- **The right to object to the processing of personal data**
- You have **the right to complain to the Information Commissioner**. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

- Transfer of Data Abroad: Please refer to our information audit for privacy shield information.
- You have **the right to object** if we process your personal data for the purposes of direct marketing.
- With some exceptions, you have **the right not to be subjected to automated decision-making**.
- You have **the right to be notified of a data security breach** concerning your personal data.
- **In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Play Alloa Office. However, if you withdraw your consent we may be unable to provide you with our service.**

9 Subject Access Requests (SAR)

9.1 Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing to the Play Alloa Office. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

9.2 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

10 Further processing

10.1 If we wish to use your personal data for a new purpose, not covered by this Data Protection Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions.

10.2 Where and whenever necessary, we will seek your prior consent to the new processing. Contact Details To exercise all relevant rights, queries of complaints please in the first instance, contact us at:

- Play Alloa
  19 Broad Street
  Alloa
  FK10 1AN

  Tel: 01259 721511

Data Breach Procedure for Play Alloa

Policy Statement
Play Alloa holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Play Alloa and all staff and volunteers, referred to herein after as 'staff'.

Purpose
This breach procedure sets out the course of action to be followed by all staff at Play Alloa if a data protection breach takes place.

Legal Context
Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
   (a) Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   (b) Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (c) Describe the likely consequences of the personal data breach;
   (d) Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Types of Breach
Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a Data Breach
In the event that the organisation identifies or is notified of a personal data breach, the following steps should followed:

1. The person who discovers/receives a report of a breach must inform the Senior Project Manager (SPM). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
2. The SPM (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.
3. The SPM (or nominated representative) must inform the Board as soon as possible. As a registered Data Controller, it is the organisation's responsibility to take the appropriate action and conduct any investigation.
4. The SPM (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.
5. The SPM (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
    a. Attempting to recover lost equipment.
    b. The use of back-ups to restore lost/damaged/stolen data.
    c. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
    d. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation
In most cases, the next stage would be for the SPM (or nominated representative) to fully investigate the breach. The SPM (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation.

The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The SPM (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the SPM (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available team meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The SPM should ensure that staff are aware of the Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the Data Protection policy and associated procedures, they should discuss this with their line manager.