Pannal Ash Junior Football Club

DATA BREACH POLICY

Scope

This Data Breach Policy (Policy) sets out how PAJFC (the Club) manages security incidents involving the destruction, loss, alteration or unauthorised disclosure of, or access to, personal data (Personal Data Breach).

The Club is committed to handling personal data securely and properly. Lawful handling of personal data consistent with this Policy is vital to supporter and volunteer trust and engagement, fundraising and research. Security incidents may pose significant risks, unless handled appropriately. Security incidents should therefore involve timely reporting, reactive, preventative and risk mitigation activities and be handled at all times in accordance with this Policy.

This Policy sits alongside other policies which relate to the use, processing and security of personal data, in particular our Privacy Policy, as well as our Data Retention policy.

The purpose of this Policy is to provide clear guidelines to all volunteers, as well as contractors, Club members and other persons having access to the Club's personal data, on how to identify and deal with a security incident involving a Personal Data Breach, which may constitute a breach of data protection laws and/or require the Club to notify:

the Information Commissioner's Office; and

for serious breaches, the impacted data subjects (e.g. volunteers, members or partners).

In certain circumstances, the Club may also be under a contractual obligation to notify other organisations of a Personal Data Breach

Definitions used within this Policy are set out in Appendix 2.

Responsibilities

It is the responsibility of all volunteers and Trustees to assist the Club to comply with this Policy. All volunteers must familiarise themselves with this Policy and comply with its provisions in the event of a Personal Data Breach, including reporting incidents appropriately and taking steps to prevent incidents from recurring.

Trustees must decide if a security incident constitutes a Personal Data Breach and advise of the legal or regulatory elements in dealing with the breach. They must notify the relevant authorities. The Trustees have ultimate responsibility for managing suspected personal data breaches. All volunteers must be aware of how to prevent a personal data breach and how to report to Trustees if one occurs.

Notification to the Supervisory Authority

The Club is required to notify a Personal Data Breach to the relevant supervisory authority within **72 hours** of becoming aware of the breach. The notification must include the following details:

- 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;
- the name and contact details of the contact point where more information can be obtained;
- the likely consequences of the Personal Data Breach;
- the measures taken or proposed to be taken by the Club to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where possible, this information should be provided at the same time. However, if further investigation is required, a reason for the delay should be communicated to the supervisory authority and the information may be provided in phases without undue delay.

The Club is required to notify a breach in all circumstances, **unless** it is of a minor nature and

therefore **unlikely to result in a risk to the rights and freedoms of natural persons**. Each case will need to be assessed by the Trustees, but a combination of some or all of the following factors **may** indicate that the breach does **not** need to be notified:

- the Personal Data Breached is publically available (e.g. business email addresses; information on a public register); **or**
- the personal data was encrypted, in a non-readable format or secured in a way which would make it technically difficult to access; **or**
- the total number of personal data records was small (as an **approximate** guide, < 20 records); **or**
- the personal data would not allow a malicious third party to commit an act of identity theft or fraud;

AND

- the breach will not result (directly or indirectly) in financial loss for any individuals; **and**
- the breach will not result in damage to an individual's reputation; **and**
- the breach will not result in loss of confidentiality of personal data protected by professional secrecy; **and**
- the breach will not result in any other significant economic or social disadvantage to the individual(s) concerned.

Notification to Data Subjects

In some circumstances, the Club may be required to notify a Personal Data Breach to the affected individuals ("**data subjects**").

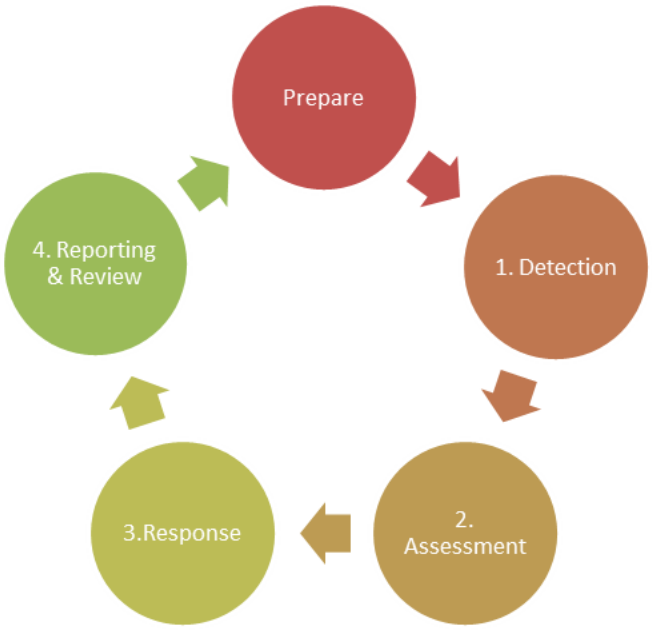
A notification to data subjects will be necessary where the breach **"is likely to result in a high risk to the rights and freedoms of natural persons."** This is a higher bar than the test for notifying a breach to the supervisory authority.

Each case will need to be assessed by the Trustees in context, and where appropriate with the guidance of external lawyers.

Detecting and Responding to a Personal Data Breach

Pannal Ash Junior Football Club

The Club has a four step approach to dealing with Personal Data Breaches involving (1) detection, (2) assessment, (3) response handling and (4) review.



Step 1 - Detection

The Club expects Personal Data Breaches to be detected through three main channels:

1. **Volunteer Reporting**

   Volunteers are expected to be mindful of potential Personal Data Breaches and immediately report concerns about any situation where a breach has or may have arisen to Trustees.
   The Club encourages openness to report actual or suspected security incidents and will not take disciplinary action against anyone who may have been involved in a security incident provided they report the breach in accordance with this Policy and where their involvement in the breach (i) was not deliberate, or (ii) was not part of a series of similar incidents involving the same person (regardless of intent).

2. **Monitoring**

   The Club monitors IT systems to detect potential security incidents and Personal Data Breaches and volunteers are expected to monitor for unusual behaviour which could indicate that someone is trying unlawfully, or without good cause or authorisation, to access files containing personal data, or to disclose that personal data outside of the Club.

3. **Third Party/External Notifications**

   If a third party (e.g. an IT provider or supplier) becomes aware of an actual or

potential security incident or Personal Data Breach, it is important that any notification provided to the Club is properly captured and assessed. Volunteers are expected to be proactive in escalating any information provided by third parties about a potential Personal Data Breaches immediately.

Step 2- Assessment
Where a Personal Data Breach is detected and notified in accordance with the above, an initial assessment will be undertaken and triage process commenced by Trustees. This will involve:

- establishing the facts of the case;
- advising on any immediate steps needed to contain the Personal Data Breach (for example, changing user passwords);
- initial consultation with external advisors, where required;
- recording the Personal Data Breach and the ongoing investigation.

Step 3 - Response
The precise action to be taken by the Trustees will depend on the nature of the Personal Data Breach. However, it is likely to include:

- **investigation**: to understand the nature of the incident, the impact on the Club (in terms of legal liability, reputational damage, financial impact, organisational impact and other risk factors) and help establish the underlying cause and establish impacted internal and external stakeholders;
- **containment**: of the breach to prevent any further data loss or security compromises, which may involve, for example, taking systems offline;
- **restoration**: of any services impacted by the breach as soon as possible once the breach has been contained, this may include recovering data from suitable backup systems provided all traces of the compromise have been removed;
- **intervention and improvement**: to existing business processes to prevent recurrence of the incident, this may be supported by targeted security awareness training or legal action;

- **preservation of evidence**: if it is decided to pursue a perpetrator of the Personal Data Breach it will be essential to take a forensic copy of the affected system immediately after the security breach was detected as evidence of the breach;
- **engagement with stakeholders**: it is important to effectively engage with those directly affected by or who may have a wider interest in management of the breach. This is likely to include volunteers, supporters, fundraisers, the media, and appropriate regulators or law enforcement agencies. An engagement plan should be agreed at the earliest opportunity and is likely to include the activities set out in the table below.

Step 4 - Incident Reporting and Review

Trustees should co-ordinate and hold a post incident review meeting. The review meeting must cover the following issues:

- did the detection and response procedures work as intended?
- if not, which areas need to be amended?
- what changes could be made to procedures to improve the ability of the Club to detect and deal with a similar incident?
- what tools worked well and what additional tools would be useful for the future?
- was the level of the Club's response appropriate?
- could any lessons be learnt from the incident? In particular, did a standard response exist for the incident or should one be developed?

Due to possible operational weaknesses which an incident may indicate, and because of the potential for damage to the Club's reputation, the Trustees should be informed of any incident which is notified to a supervisory authority.

It may be appropriate for the output of the post-incident review to be written up in the form of an incident report, and kept by the Club on file for reference. The incident report should be shared with the Trustees, who should be expressly reminded of the confidential nature of the document.

Pannal Ash Junior Football Club

APPENDIX 1
PAJFC POLICIES RELATING TO THE PROCESSING OF PERSONAL DATA

1. Privacy Policy

2. Data Retention Policy

APPENDIX 2
DEFINITIONS

"Data Controller" shall mean the person or company who, either alone or jointly with others, determines the purpose for which, and the manner in which, Personal Data is Processed;

"Data Processor" shall mean the person or company who Processes Personal Data on behalf of the Data Controller;

"Data Subject" shall mean an identified or identifiable natural person whose Personal Data is being Processed;

"Personal Data" shall mean any information capable of identifying a natural person, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their his or her physical, physiological, mental, economic, cultural or social identity. Data is considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot make that link;

"Personal Data Breach" shall mean a security incident which involves an unauthorised or inappropriate disclosure of Personal Data; and

"Processing" shall mean any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, including, but not limited to collection, recording, organisation, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure, or destruction (and **"Process"**, **"Processes"** and **"Processed"** shall be interpreted accordingly).