SALE SHARKS DATA BREACH POLICY

This policy applies to:

All employees, workers, volunteers, contractors, consultants, and third parties who process personal data on behalf of Sale Sharks

---

1. Policy Statement

Sale Sharks is committed to protecting the personal information of its employees, supporters, season ticket holders, members, customers, suppliers, and business partners.

This policy establishes the procedures for identifying, reporting, managing, investigating, and learning from personal data breaches. Sale Sharks recognises its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 to ensure that personal data is protected against unauthorised access, disclosure, loss, alteration, or destruction.

All staff have a responsibility to report actual, suspected, or potential data breaches immediately.

---

2. Purpose

The purpose of this policy is to:

- Protect personal data held by Sale Sharks.
- Ensure a prompt and effective response to data breaches.
- Minimise harm to affected individuals.
- Meet legal and regulatory reporting obligations.
- Reduce the risk of future incidents through investigation and corrective action.
- Promote a culture of information security and accountability.

---

3. Scope

This policy applies to all personal data processed by Sale Sharks, including information relating to:

- Employees and job applicants.

- Supporters and season ticket holders.
- Members and customers.
- Volunteers and contractors.
- Suppliers and business contacts.

The policy applies to personal data held in any format, including:

- Electronic records.
- Emails and digital communications.
- Paper records.
- Portable devices.
- Audio and video recordings.
- Photographs and images.

---

4. Definition of a Personal Data Breach

A personal data breach is any security incident that results in the accidental or unlawful:

- Destruction of personal data.
- Loss of personal data.
- Alteration of personal data.
- Unauthorised disclosure of personal data.
- Unauthorised access to personal data.

A breach may occur through human error, system failure, malicious activity, theft, or accidental disclosure.

---

5. Examples of Data Breaches

Examples include, but are not limited to:

- Sending personal information to the wrong recipient.
- Losing paper files containing personal information.

- Losing a laptop, mobile phone, USB device, or other equipment containing personal data.
- Unauthorised access to a database or system.
- Sharing personal information with someone who is not authorised to receive it.
- Cyber-attacks, ransomware, malware, or phishing incidents.
- Failure to securely dispose of confidential records.
- Publishing personal information accidentally on a website or social media platform.
- Theft of records or equipment containing personal data.

---

6. Responsibilities

All Employees, Volunteers and Contractors

All individuals handling personal information must:

- Protect personal data at all times.
- Follow Sale Sharks data protection and information security procedures.
- Report actual, suspected, or potential data breaches immediately.
- Cooperate with investigations into security incidents.
- Complete mandatory data protection and cyber security training.

Managers

Managers are responsible for:

- Ensuring staff understand their responsibilities.
- Escalating reported breaches immediately.
- Supporting investigations and corrective actions.
- Promoting compliance with this policy.

Data Protection Officer (DPO) or Designated Responsible Person

The designated Data Protection Officer or responsible manager will:

- Assess reported incidents.
- Determine the level of risk.

- Coordinate breach investigations.
- Maintain a breach register.
- Determine whether regulatory notification is required.
- Recommend corrective and preventative actions.

---

7. Reporting a Data Breach

All actual, suspected, or potential breaches must be reported immediately.

Where a breach is identified, employees must:

Step 1 - Contain the Incident

Where possible:

- Prevent further disclosure of information.
- Retrieve incorrectly shared information.
- Secure affected systems or records.
- Change passwords if system access may be compromised.

Step 2 - Report the Incident

Report the incident immediately to:

- Your line manager.
- The Data Protection Officer (DPO) or designated responsible manager.

Employees must not attempt to conceal a breach.

Step 3 - Record Key Information

Provide details including:

- Date and time of the incident.
- Nature of the breach.
- How the incident occurred.
- Categories of data involved.
- Number of individuals affected.
- Immediate actions taken.

- Any known risks to affected individuals.

---

8. Breach Assessment

Following notification, Sale Sharks will assess:

- The type and sensitivity of information involved.
- The volume of data affected.
- The number of individuals impacted.
- Whether the data was encrypted or otherwise protected.
- The likelihood of harm to individuals.
- Any legal, financial, operational, or reputational risks.

The outcome of the assessment will determine the appropriate response.

---

9. Breach Response Procedure

Stage 1 – Containment and Recovery

Sale Sharks will take immediate steps to:

- Stop the breach from continuing.
- Recover lost information where possible.
- Secure systems and records.
- Prevent further unauthorised access.

Stage 2 – Investigation

A formal investigation will be undertaken to determine:

- What happened.
- When the breach occurred.
- The root cause of the incident.
- The extent of the breach.
- Whether policies or procedures were followed.

Stage 3 – Corrective Action

Where necessary, Sale Sharks will implement measures such as:

- System security improvements.
- Staff retraining.
- Process improvements.
- Additional access controls.
- Policy updates.

---

10. Notification Requirements

Where a personal data breach presents a risk to the rights and freedoms of individuals, Sale Sharks may be required to notify the Information Commissioner's Office (ICO).

Where a breach is likely to result in a high risk to affected individuals, Sale Sharks may also notify those individuals directly.

Notifications will be made by the Data Protection Officer or an authorised member of management.

---

11. Breach Register

Sale Sharks will maintain a Data Breach Register recording:

- The date of the incident.
- Nature of the breach.
- Data affected.
- Individuals impacted.
- Risk assessment findings.
- Actions taken.
- Notification decisions.
- Lessons learned.

All breaches, regardless of severity, should be recorded.

---

12. Training and Awareness

Sale Sharks will provide regular training and awareness activities to ensure employees understand:

- Data protection responsibilities.
- Safe handling of personal information.
- Cyber security risks.
- How to recognise and report breaches.
- Incident response procedures.

Additional training may be provided following significant incidents.

---

13. Non-Compliance

Failure to comply with this policy may result in:

- Disciplinary action.
- Withdrawal of system access.
- Termination of employment or contracts.
- Legal or regulatory action where appropriate.

Intentional misuse or unauthorised disclosure of personal information may be treated as gross misconduct.

---

14. Monitoring and Review

Sale Sharks will review this policy annually or sooner where:

- Legislation or regulatory guidance changes.
- Significant organisational changes occur.
- A serious breach or security incident highlights areas for improvement.
- New risks to personal data are identified.

Policy Approval

Policy Owner: Chief Executive Office/Head of People & Change/Governance Manager

Approved By: Board of Directors

Effective Date: 1st August 2026

Review Date: 31st July 2028

Sale Sharks is committed to responding quickly, effectively, and transparently to any data breach and to protecting the personal information of staff, supporters, customers, and other stakeholders.