

Data Protection & Incident Policy

Last updated: 09:10 08/06/2026



Purpose

As a platform facilitating interactions between Scouts of varying ages, ScoutSwap C.I.C. handles sensitive personal data including email and physical addresses, dates of birth, geolocation, and safeguarding reports. This policy outlines how all volunteers, management, and directors must handle this data to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It also serves as our formal Incident Response Plan in the event of a data breach.

Scope

This policy applies to all ScoutSwap team members. "Data" refers to any information that can identify a living person, including users, volunteers, and staff.

Routine Data Handling Rules

Safe Handling Procedures for Sensitive Information

When your role requires accessing sensitive information (e.g., verification photos, age data, or safeguarding reports), you must adhere to these strict protocols:

- **Verify your environment:** Before opening any sensitive file or dashboard, ensure you are in a private environment where no unauthorized third parties (family members, friends, or strangers) can view your screen.
- **Minimise exposure:** Only keep the necessary data window open for the minimum time required to complete your task. Close the tab or window immediately after the check is complete.
- **Clean desk policy:** Ensure no physical notes containing user information are left on your desk. If you must take a note, it must be stored securely and destroyed (cross-cut shredded or burnt) immediately after the task is concluded.
- **No multi-tasking:** Do not switch between sensitive ScoutSwap data and personal applications or public websites while handling sensitive information. This prevents accidental copy-pasting of private user data into public chat windows.
- **Report unintended exposure:** If you accidentally display sensitive data on a public screen or within an unauthorized communication channel, you must report this as a potential breach immediately, even if no harm occurred.

Communication and System Security

- **Official channels:** All ScoutSwap business must be conducted via official [name]@scoutswap.co.uk email addresses or the secure internal Discord server. Use of personal email or social media accounts for official ScoutSwap business is prohibited.

Data Protection & Incident Policy

Last updated: 09:10 08/06/2026



Routine Data Handling Rules

- **Screenshots and logging:** Do not take screenshots of user profiles or verification screens unless requested by management for evidence logging. If a screenshot is taken for this purpose, it must be deleted immediately after it is uploaded to the secure internal staff channel.
- **Account security:** Volunteers must use strong, unique passwords and enable Two-Factor Authentication (2FA) on all accounts accessing ScoutSwap infrastructure, where available.

Do not delete official correspondence, support tickets, or user reports. Deletion of official records is handled exclusively by management in accordance with our documented Data Retention and Safeguarding Policies.

Data Breach & Incident Response Plan

Defining a Breach

A personal data breach is any security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Examples include:

- Sending user information to the wrong recipient.
- A volunteer's Discord account being compromised.
- Leaving an administrative dashboard exposed on a public terminal.

Response Procedure

Stage	Responsibility	Action
1: Report	All staff	Report suspected breaches immediately via an emergency Discord ticket, email or phone call.
2: Contain	Directors	Disable compromised accounts and restrict access privileges immediately.
3: Assess	Directors	Evaluate the volume, sensitivity, and risk to the affected individuals.
4: Notify	Directors	Notify the ICO within 72 hours if the breach poses a risk to individuals; notify users if the breach poses a "high risk".
5: Review	Directors	Conduct a post-incident review to update policies and patch vulnerabilities.

Data Protection & Incident Policy

Last updated: 09:10 08/06/2026



Record Keeping

ScoutSwap C.I.C. maintains a formal internal breach register. This log includes the facts relating to the breach, its effects, and the remedial actions taken, ensuring full transparency for governance and potential regulatory review.

Review and Responsibility

This policy will be reviewed periodically to ensure it remains effective, legally compliant, and aligned with best practice governance for Community Interest Companies.

Last review: Jun 2026

Next review: Jun 2027

Approval

Approved by the directors on 08/06/2026.

Joe Biondani
Director

Oscar Grothusen
Director