IAF Data Breach Policy & Procedure

1. Purpose

The Inspire and Achieve Foundation (IAF) is committed to protecting the personal data of beneficiaries, staff, volunteers, and partners. This policy sets out how IAF identifies, reports, investigates, and responds to personal data breaches in line with:

- **UK GDPR**
- **Data Protection Act 2018**
- **ICO guidance on personal data breaches**

A consistent and timely response reduces harm to individuals, protects IAF's reputation, and ensures legal compliance.

2. Scope

This policy applies to:

- All personal and special category data held by IAF
- All staff, volunteers, trustees, contractors, and data processors
- All systems and formats (electronic, paper, audio, images, messaging platforms, cloud storage)

It covers **confirmed and suspected** data breaches.

3. Definitions

Personal Data Breach

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

Examples include:

- Lost or stolen laptops, phones, USBs, or paper files
- Sending personal data to the wrong person
- Unauthorised access to SharePoint or email
- Hacking, malware, or phishing attacks
- Accidental deletion of records
- Staff discussing personal data inappropriately
- Failure of IT systems resulting in data loss
- Sharing more information than necessary with a partner agency

High-risk breaches

Breaches likely to result in significant harm to individuals, such as:

- Identity theft
- Financial loss
- Safeguarding risk
- Discrimination
- Reputational damage
- Exposure of sensitive health or offending information

4. Roles and Responsibilities

Data Protection Lead (DPL)

- Oversees breach management
- Assesses risk and determines reportability
- Notifies the ICO within 72 hours if required
- Notifies affected individuals where necessary
- Maintains the breach log
- Leads post-incident reviews

Investigating Officer (IO)

Appointed depending on the nature of the breach (e.g., Manager, IT provider).
Responsible for:

- Fact-finding
- Containment actions
- Recovery steps
- Recommendations

All Staff and Volunteers

- Must report breaches **immediately**
- Must not attempt to hide or resolve breaches alone
- Must cooperate with investigations

5. Identifying a Breach

A breach may be identified by:

- A staff member noticing an error
- A beneficiary reporting a concern
- IT systems alerting to unusual activity
- A partner organisation notifying IAF
- A lost device or file
- Suspicious emails or cyber-attack indicators

If in doubt, **treat it as a breach** and report it.

6. Reporting a Breach

Immediate action required

All staff must report suspected or confirmed breaches **as soon as they become aware**, using:

craig.stevens@inspireachieve.co.uk
(or the Director if the DPL is unavailable)

Reports must include:

- What happened
- When it happened
- Who is affected
- What data is involved
- Any actions already taken

A Data Breach Report Form must be completed.

7. Containment and Recovery

The DPL will immediately assess whether the breach is ongoing. Actions may include:

- Revoking system access
- Resetting passwords
- Contacting IT support (Gilford Computing)
- Recovering lost devices
- Requesting deletion from unintended recipients
- Securing physical files
- Isolating compromised systems

The priority is to **limit harm** and **prevent further loss**.

8. Investigation and Risk Assessment

An investigation will begin **within 24 hours** of the breach being reported.

The IO will assess:

8.1 Nature of the data

- Is it personal or special category?
- Does it include health, offending, or safeguarding information?

8.2 Volume of data

- How many individuals are affected?
- How much information was exposed?

8.3 Sensitivity

- Could the data cause harm, distress, or risk?

8.4 Security measures

- Was the data encrypted, password-protected, or anonymised?

8.5 Potential consequences

- Safeguarding risk
- Identity theft
- Reputational damage
- Loss of trust
- Financial loss

The IO will produce a written assessment for the DPL.

9. Notification Requirements

9.1 Reporting to the ICO

IAF must notify the ICO **within 72 hours** if the breach is likely to result in a **risk to the rights and freedoms of individuals**.

The notification will include:

- Nature of the breach
- Categories and volume of data
- Number of individuals affected
- Likely consequences
- Containment and mitigation actions
- Contact details for the DPL

If the breach does not meet the threshold, it will still be recorded internally. Where a decision is taken not to notify the ICO, the rationale for that decision will be documented within the Data Breach Log.

9.2 Notifying Individuals

Affected individuals must be informed **without undue delay** if the breach is likely to result in **high risk**, such as:

- Exposure of health or mental health information
- Offending history
- Safeguarding concerns
- Identity documents

- Financial information

Notifications will include:

- What happened
- What data was involved
- What IAF has done to contain the breach
- What individuals can do to protect themselves
- Who to contact for support

9.3 Notifying Other Parties

Where relevant, IAF may notify:

- Police
- Funders
- Insurers
- Partner agencies
- IT providers

10. Recording Breaches

IAF maintains a **Data Breach Log** containing:

- Date and time of breach
- Description of incident
- Individuals affected
- Risk assessment
- Actions taken
- Whether the ICO was notified
- Lessons learned

All breaches — even minor ones — must be logged. Data breach records will be retained for a minimum of six years from the date of the incident.

11. Evaluation and Learning

After containment, the DPL and SMT will conduct a review to identify:

- Root causes
- Whether policies or procedures need updating
- Whether staff training is required
- Whether technical controls need strengthening
- Whether the breach indicates wider systemic issues

A written report will be produced for trustees where appropriate.

12. Training and Awareness

All staff and volunteers receive:

- Induction training on data protection and breach reporting
- Annual refresher training
- Additional training for high-risk roles

13. Policy Review

This policy will be reviewed every **two years**, or sooner if:

- Legislation changes
- New risks emerge
- Systems or processes change