# INDEPENDENT SCHOOLS INSPECTORATE
# PERSONAL DATA BREACH POLICY

| | |
|---|---|
| **DATE OF POLICY:** | **August 2025** |
| **POLICY OWNER:** | **Chief Operating Officer** |
| **APPROVED BY:** | **Chief Executive Officer – Chief Inspector** |
| **DATE TO BE REVIEWED:** | **August 2027** |

**Policy statement**

1. Personal data breaches can impact the rights and freedoms of data subjects.

2. Under the UK General Data Protection Regulation (UK GDPR) and the associated UK data protection legislation, ISI has a duty to report a personal data breach which is likely to result in a risk to the rights and freedoms of the concerned individuals to the Information Commissioner's Office (ICO) without undue delay and **no later than 72 hours after becoming aware of it.** This is a legal requirement.

3. All users of @isi email addresses (e.g. Board members and contractors), ISI employees, contractors working on behalf of ISI, and all inspectors (reporting and team inspectors) are obliged to comply with this policy.

4. The Chief Operating Officer (COO) has overall responsibility for compliance with this policy and managing data breaches, but the implementation may be delegated to appropriately trained individuals including the Director with responsibility for compliance with regulatory requirements or the lead person responsible for governance. References made to any actions to take or decisions to make by the COO include these other delegated roles. If either the COO or relevant Director are unavailable, decisions may be made by Chief Executive Officer-Chief Inspector (CEO-CI) and/or the lead person responsible for governance.

**How to recognise a personal data breach**

5. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that result from accidental and/or deliberate action. It also means that a breach is about more than just losing personal data.

6. Personal data breaches can include:
    i. access by an unauthorised third party;
    ii. deliberate or accidental action (or inaction) by a controller or processor;
    iii. sending personal data to an incorrect recipient;
    iv. computing devices containing personal data being lost or stolen;
    v. alteration of personal data without permission; and
    vi. loss of availability of personal data.

7. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

**Personal data breach response**

8. If it is suspected that a personal data breach has occurred, the following steps must be taken:

    i. Report the breach immediately to the COO, copying in dp@isi.net, stating when the breach was discovered and providing a brief outline of the suspected breach taking care not to repeat any personal information that may lead to a further or repeated breach.

ii. The COO (with advice as appropriate) will promptly decide whether a breach has occurred and whether this is likely to result in a risk to the rights and freedoms of the individuals concerned. In the absence or unavailability of the COO or the other roles noted in paragraph 4 above, the CEO-CI will decide based on the information provided by the delegated person.

iii. If it is deemed that a breach has occurred which is likely to result in a risk to the rights and freedoms of the individuals concerned, the COO is responsible for ensuring the breach is reported to the ICO **without undue delay, but not later than 72 hours after the initial discovery of the breach**. (This action may be delegated to another member of staff but, if so, the COO must ensure that it has been carried out and within the required time scale.)

iv. Not all breaches need be reported to the ICO (although all breaches will still be recorded). A breach **is** reportable if likely to cause harm[1] to individuals– either due to the nature of the data (eg sensitive personal data), the nature of the individuals concerned (eg a child or vulnerable person), or the volume of the data (eg a thousand people are concerned).

9. In the event of making a referral, the following information must be provided to the ICO:
   i. a description of the nature of the personal data breach including, where possible:
      a. the categories and approximate number of individuals concerned; and
      b. the categories and approximate number of personal data records concerned;
   ii. the name and contact details of the COO as the point of contact from whom more information can be obtained;
   iii. a description of the likely consequences of the personal data breach; and
   iv. a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects;
   v. if the provision of full details within 72 hours is not feasible, explain the delay to the ICO and provide a timeframe within which further information will be submitted.

10. Note that if a breach affects individuals in different European Economic Area countries, the ICO may not be the lead supervisory authority. The COO will establish which European data protection agencies would be the lead supervisory authority for the processing activities that have been subject to the breach.

**Telling individuals about a breach**

11. If a breach is likely to result in a high risk to the rights and freedoms of individuals, ISI must inform those concerned directly and without undue delay. The threshold for informing individuals is higher than for notifying the ICO. The COO, with advice as appropriate from the Head of Information Technology, will assess the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, ISI will promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. Note that one of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

12. If ISI decides not to notify individuals, ISI will still need to notify the ICO unless it can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. Note that the ICO has the power to compel ISI to inform affected individuals if the ICO considers there is a high risk. In any event, ISI will document the decision-making process.

[1] ICO Overview of data protection harms and the ICO's taxonomy

**What information will be provided to individuals when telling them about a breach**

13. If it is decided that data subjects need to be contacted in relation to a breach, they should be provided with the following information:
    i. the name and contact details of the COO as the point of contact from whom more information can be obtained;
    ii. a description of the likely consequences of the personal data breach; and
    iii. a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

14. If possible, ISI will give specific and clear advice to individuals on the steps they can take to protect themselves, and what ISI is willing to do to help them. Depending on the circumstances, this may include such things as:
    i. Forcing a password reset;
    ii. Advising individuals to use strong, unique passwords; and
    iii. Telling them to look out for phishing emails or fraudulent activity on their accounts.

**Documenting breach responses**

15. All breaches must be reported internally (as set out above), regardless of whether they need to be reported to the ICO.

16. The COO will ensure that the facts relating to the breach, its effects and the remedial action taken, including reasons for decisions, are all documented.

17. The COO will ensure the breach is thoroughly investigated (whether personally or delegating), including whether the breach was a result of human error or a systemic issue and how a recurrence can be prevented through better processes, further training or other corrective steps.

18. Any breaches reported to the ICO will also be reported to the ISI Board.

**Further notifications**

19. The COO will consider notifying third parties such as the police, insurers, and professional bodies.

**Reducing the likelihood of data breaches**

20. Human error is the leading cause of reported data breaches. To reduce the risk of this, ISI will implement:
    - mandatory data protection induction and refresher training;
    - updating policies and procedures;
    - ensuring employees feel able to report incidents of near misses;
    - working to a principle of “check twice, send once”;
    - investigating the root causes of breaches and near misses;
    - Restricting access and auditing systems;
    - Implementing technical and organisational measures.

| Contact details for reporting a breach | | |
|---|---|---|
| **Email both of these addresses as soon as possible on discovery of a breach:** | | |
| Chief Operating Officer | John Timothy | John.timothy@isi.net |
| Head of Governance | Kirstin Stansfeld | Kirstin.stansfeld@isi.net |
| Please copy in dp@isi.net and providing a brief outline of the suspected breach, taking care not to repeat any person information that may lead to a further or repeated breach | | |
| ISI general reception telephone: 0207 600 0100 during business hours | | |

**TABLE OF KEY CHANGES**

| Date of review | Paragraph | Amendments |
|---|---|---|
| **August 2025** | All | Updated job roles and responsibilities |
| | 4 | Updated to provide clarity on responsibilities and delegation(s) |
| | 8 | Note to cc dp@isi.net when reporting a suspected breach and clarity on reporting processes and delegations for action |
| | 5, 7, 10, 11, 12, 15 | Revised/additional paragraphs reflecting compliance with ICO guidance / requirements |
| | 18 | Clarity that any breaches reported to the ICO will be reported to the ISI Board |
| | 20 | Updated contact details for reporting a breach |