Personal Data Breach Procedure

Reference: GCSB-POL-008
Version: 1.0
Issuing authority: Global Converged Security Board
Effective: 13 October 2026

1. Purpose and scope

This Procedure sets out how the Global Converged Security Board (GCSB) responds to a personal data breach under the UK GDPR and the Data Protection Act 2018. It applies to every office holder, board, committee and panel member, editor and peer reviewer, and to every system holding personal data: the public register, member accounts, role applications and CVs, Journal manuscripts and reviews, Trustmark and partner applications, profile photos and email.

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

2. Reporting a suspected breach

Anyone who suspects a breach reports it immediately, and in any case within 24 hours, to info@gcsb.uk with the subject "Data breach". The Data Protection Officer registered with the ICO (info@gcsb.uk) acts as Data Protection Lead. Do not try to investigate alone, delete evidence or contact the people affected before the breach is assessed.

3. Contain

The Data Protection Lead acts at once to stop the breach and limit harm: for example revoking access, rotating credentials or keys, withdrawing a document link, recalling an email or asking a recipient to delete data.

4. Assess the risk

The Data Protection Lead records what data and whose data is involved, how many people, how it happened, and the likely consequences for them. Special attention is given to CVs, manuscripts under review, reviewer identities, contact details and payment evidence.

5. Notify the ICO within 72 hours

Unless the breach is unlikely to result in a risk to people's rights and freedoms, GCSB notifies the Information Commissioner's Office without undue delay and no later than 72 hours after becoming aware of it. If full details are not yet known, an initial report is made and completed later. Reasons for any delay are recorded.

6. Tell the people affected

Where the breach is likely to result in a high risk to people, GCSB tells them without undue delay, in plain language: what happened, the likely consequences, what GCSB has done and what they can do to protect themselves, with a contact point. Where the identity of a double-blind reviewer or author is exposed, the editor is also informed so the review can be protected.

7. Record and learn

Every breach, including those not reported to the ICO, is recorded in the breach log: facts, effects, decisions and actions taken. The Audit & Risk Committee reviews the log and any lessons learned, and the Data Protection Lead tracks the agreed improvements.

8. Service providers

GCSB's hosting, database and email providers must tell GCSB without undue delay of any breach affecting GCSB data. GCSB then follows this Procedure.

9. Policy control

- Approval authority: Governing Council, on the recommendation of the Audit & Risk Committee.
- Revision history: version 1.0 (13 October 2026) first issue.
- Review date: reviewed at least once a year and after any reportable breach; next review no later than 13 October 2027.
- Precedence: this Procedure is subordinate to the Governance Charter (GCSB-POL-001) and the Privacy Policy, and never overrides statutory duties under data protection law.

© 2026 Global Converged Security Board. All rights reserved.