PROVINCIAL GRAND LODGE OF CORNWALL

The following document establishes the formal procedures for the Provincial Grand Lodge of Cornwall to respond to any actual or suspected Personal Data Breach, ensuring compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

DATA BREACH INCIDENT MANAGEMENT PLAN
PROVINCIAL GRAND LODGE OF CORNWALL

Key Roles & Contact	Name/Title	Contact Details
Data Protection Officer (DPO)	Provincial Grand Registrar	Email: registrar@pglcornwall.org.uk (Initial Report)
Provincial Grand Master (PGM)	Provincial Grand Master **Senior Management Consultation**	Provgsec@pglcornwall.org.uk
Provincial Grand Secretary (PGS)	Provincial Grand Secretary **Operational Lead/Coordination**	Provgsec@pglcornwall.org.uk
Provincial Office Address	N/A	7 New Bridge Street, Truro, Cornwall TR1 2AA

1. Definitions and Breach Source Classification

A Personal Data Breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Breach Type	Description	Primary Data Controller Responsible
Local Breach	Affects data stored locally by the Province or a Lodge (e.g., lost physical files, misdirected email, unsecured local spreadsheet, compromised officer's laptop).	Province of Cornwall (or the Lodge)
Systemic Breach	Affects the central HERMES platform or UGLE-managed infrastructure where the bulk of member data is stored.	UGLE (as Data Processor)

2. Phase 1: Detection and Initial Containment (T + 0 to T + 1 Hour)

The immediate goal is to contain the breach and notify the Provincial DPO.

Step	Action by (Initial Reporter – any member/officer)	Timeframe
2.1 Discover/Detect	Identify the breach or suspicion.	T + 0
2.2 CONTAINMENT ACTION	**For LOCAL Breach (E.g., Laptop Lost):** Isolate the affected item/system (e.g., turn off the computer, revoke local access, recall the misdirected email). **For SYSTEMIC Breach (E.g., HERMES appears compromised): Do NOT** attempt to log in or fix the system. Immediately log out and await instructions from the Provincial DPO/UGLE.	Within Minutes

Provincial Grand Lodge of Cornwall
7, New Bridge Street, TRURO, TR1 2AA
Telephone: 01872 276191. Email: secretary@pglcornwall.org.uk
www.pglcornwall.org.uk @CornwallMason Provincial Grand Lodge of Cornwall https://solomon.ugle.org.uk/

Step	Action by (Initial Reporter – any member/officer)	Timeframe
2.3 Internal Notification	Report the incident immediately to the Provincial Grand Secretary (PGS) and the Data Protection Officer (DPO). **Use the most secure and immediate method** (e.g., phone call followed by encrypted email).	T + 1 Hour

3. Phase 2: Investigation and Notification Flow (T + 1 to T + 24 Hours)

The DPO and PGS lead the investigation to determine the severity and scope. The notification procedure differs based on the source:

A. Local Breach Investigation (Lodge/Province Responsibility)

Step	Action by (DPO/PGS Lead)	Timeframe
3.1 Record Incident	Start a comprehensive log (what, where, when, who discovered it, specific data categories affected, number of data subjects).	Immediate
3.2 Risk Evaluation	Assess the risk to members' rights and freedoms (financial loss, identity theft, reputational damage).	T + 12 Hours
3.3 Stakeholder Consultation	Consult with the Provincial Grand Master before deciding on external reporting.	T + 24 Hours

B. Systemic Breach Investigation (UGLE Processor Responsibility)

Step	Action by (DPO/PGS Lead)	Requirement (from DPA Schedule)
3.4 Processor Notification	The Province awaits notification **from UGLE (as Processor)** stating that a breach has occurred within the HERMES system.	UGLE must notify the Province "without undue delay."
3.5 Controller Awareness	The 72-hour clock for ICO reporting **starts the moment the Provincial DPO becomes aware** of the breach, whether by internal detection or by notification from UGLE.	Immediate
3.6 Information Reliance	The Province relies on UGLE to provide details on the nature of the breach, its scope, and the initial containment measures taken on the HERMES platform.	Continuous

4. Phase 3: External Reporting (T + 24 to T + 72 Hours)

Provincial Grand Lodge of Cornwall
7, New Bridge Street, TRURO, TR1 2AA
Telephone: 01872 276191. Email: secretary@pglcornwall.org.uk
www.pglcornwall.org.uk @CornwallMason Provincial Grand Lodge of Cornwall https://solomon.ugle.org.uk/

This phase focuses on the two mandatory external notifications under UK GDPR.

Action	Action by (DPO with PGM/PGS approval)	Statutory Deadline
4.1 Report to ICO	**IF** the breach is likely to result in a risk to individuals' rights and freedoms (regardless of whether it's local or systemic). The report must include the nature of the breach, its consequences, and measures taken.	**Within 72 Hours of Awareness**
4.2 Notify Affected Members	**IF** the breach is likely to result in a **HIGH RISK** to individuals' rights and freedoms (e.g., loss of sensitive disciplinary data, large-scale contact data theft from HERMES).	**Without undue delay**

5. Phase 4: Remediation and Review (Post-72 Hours)

Step	Action by (DPO/PGS Lead and Relevant Staff)	Timeframe
5.1 Remediation (Local)	Implement changes to local protocols (e.g., better password management, encrypted storage) to prevent recurrence of Local Breaches.	Immediate/Ongoing
5.2 Remediation (Systemic)	Record the measures UGLE (as Processor) has implemented on the HERMES system to prevent the breach from recurring.	As advised by UGLE
5.3 Full Documentation	Document the complete log of the incident, its effects, and the remedial action taken (required for accountability, regardless of ICO reporting).	Finalised within 30 Days
5.4 Policy Review	Review and update this Data Breach Response Plan based on the lessons learned from the incident.	Within 60 Days

Provincial Grand Lodge of Cornwall
7, New Bridge Street, TRURO, TR1 2AA
Telephone: 01872 276191. Email: secretary@pglcornwall.org.uk
www.pglcornwall.org.uk @CornwallMason Provincial Grand Lodge of Cornwall https://solomon.ugle.org.uk/