Data breach policy 2026

Owner: CEO

Approval Level: Board

Review date: January 2028

Version: 1

Signed _____

Role _____

Date _____

Introduction & Scope

The data breach policy ensures compliance, with the protection of individual rights, and ensures organisational accountability.

This policy identifies the governing obligations and principles that Pace adheres to with regard to Data Breach and the roles and responsibilities of staff and dependent principals in accordance with the **UK GDPR** and **Data Protection Act 2018**. It should be read in conjunction with the Data Protection Policy, Data Retention Policy and the Stakeholder Privacy policies.

This document does not include procedural instructions or processes and applies to all employees, contractors, trustees, and third parties acting on behalf of Pace.

Definitions

Data: information that can be used to identify an individual, either directly or indirectly.

Data breach: accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

Data Controller: the organisation that collects and retains personal data for organisational purposes.

Data Subject: the individual to whom the data belongs.

Data Processor: a third party that processes personal data on behalf of the Data Controller and under their documented instructions.

DPIA: Data Protection Impact Assessment.

High-Risk data breach: a high-risk data breach is one that is likely to result in significant harm to the rights and freedoms of individuals, including financial, physical, psychological, or reputational harm.

Personal Data: means any information relating to an identified or identifiable natural person ("data subject").

An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.

Special Category Data: means personal data that reveals or relates to any of the following:

- racial or ethnic origin

- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data used for identification
- data concerning health
- data concerning a person's sex life or sexual orientation

Roles & Responsibilities

Data Protection Officer: CEO - the DPO operates independently of the role of the chief executive when addressing data protection issues.

The DPO is responsible for:

- Timely involvement & internal coordination
- Risk assessment and notification guidance
- Liaising with Information Commissioner's Office (ICO) and assisting individuals
- Ensuring GDPR compliance and maintaining documentation
- Leading reviews and recommending improvements

Pace Staff:

- Complete annual training for Data Protection
- Maintain diligence in compliance, data sharing, and communication
- Report all data breach incidents immediately
- Maintain compliance with Data Protection Policy, including IT usage, hard copy storage and digital data sharing and storage processes

Head of Operations:

- Ensures appropriate technical and organisational measures are in place

Risk Assessment Principles

Data breaches must be assessed, using the ICO Self-assessment to determine the risk and impact on the rights and freedoms of individuals of a data breach on the individual and the organisation.

Use the Personal data breach examples | ICO to help define the level of risk of the data breach.

Assessment must be completed as soon as the breach is identified.

Appropriate actions resulting from the data breach assessment will be defined with regards to:

- Escalation – Is the breach a High-Risk data breach and who should be informed of the breach, such as the data subject, the ICO, trustee, data processors and staff
- Communication – information that should be shared with the identified stakeholders
- Containment – what actions need to be taken to prevent further loss, both immediate and future

Assessments and associated communications must be actioned within 72 hours of the identification of the breach. Containment action must be initiated within 72 hours.

All evidence will be captured and used during escalation; it will also be reviewed for adjustment and training by the DPO.

Notification Obligations

- Notification decisions are determined by the outcome of the ICO data breach self-assessment
- Notification to the data subject, in line with the outcomes of the risk assessment, without undue delay (24 hrs), to include nature of breach, data affected, mitigation steps and contact details of the DPO
- Notify ICO within 72 hours if required

Record-Keeping Commitment

- All data breaches are reported to the DPO
- All **data breaches** are recorded on the data breach register by the individual who identifies the breach
- All **actions** are recorded on the data breach register by the DPO
- All risk assessments are stored on the GDPR SharePoint
- Records are retained in line with the Data Retention Policy

Training & Awareness Commitment

- Appropriate technical and organisational security measures are implemented and maintained by the outsourced IT department
- Systems are backed up nightly by the outsourced IT department
- Systems must have 2-step verification
- Cloud-based systems must be GDPR compliant
- Staff are trained annually on GDPR and are aware of their duties and obligations
- Any major breaches will be assessed, DPIAs and breach risk assessments will be audited in line with ISO9001:2015 standards, committing to a cycle of continuous improvements

Data Processors

- Data processors and systems are reviewed and aligned with the Pace Policy at the point of contract renewal
- Processing agreements are in place

- Processors are captured on a register with start date and end date recorded

Data processors include:

- Management Information Systems (MIS)
- Cloud & productivity platforms
- Learning platforms & EdTech tools
- IT support & managed service providers
- Safeguarding, monitoring & filtering services
- Assessment, exams & reporting
- Finance, payroll & HR services
- Clinical management services
- CRM Systems
- Communications & engagement tools

Appendix 1

Notification of data breach

Date of breach	
Date breach identified	
Assessment completion date	
Name of Assessor	
Nature of breach	
Data affected	
Level of Risk	
Stakeholders to be notified	
Contact details of the DPO	
ICO informed?	
Containment actions taken	
Notes	