GORSE

The GORSE Academies Trust Data-Breach Management Policy

Designated Person:	Strategic Lead Officer
Reviewed by:	Policy Committee
Date:	05/06/2024
Version	1.1

The GORSE Academies Trust, c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA **Chief Executive Officer:** Sir John Townsley BA (Hons) NPQH
Deputy Chief Executive Officer: Mrs L Griffiths BSC (Hons) NPQEL
Chair of the Board: Mrs A McAvan BA (Hons) NPQH

GORSE

Data-Breach Management Policy

The following amendments have been made to this (2024) version of the policy:

Full Document	Change TGAT to GORSE
Full Document	Minor grammatical updates or corrections
Section 2	2.1 Correction to source of definition and guidance

This policy should be read in conjunction with the following policies:

- GORSE IT Security Policy
- GORSE Data-Protection Policy
- GORSE Homeworking Policy
- GORSE Clear Desk & Clear Screen policy
- GORSE Information Security Policy
- GORSE Data-Privacy Impact Assessment Policy

1. Overview

1.1 This Data-Breach Management Policy applies to The GORSE Academies Trust (GORSE) including all trust establishments and central functions associated with the trust.

This policy defines:

- What is a Data-Breach
- Actions for reporting
- Actions to manage recovery
- Actions to reduce risk
- Actions to review and mitigate further instances

1.2 The policy is held on the GORSE Trust Drive, within the Policies section and should be reviewed every 3 years, or if other polices/legislation determine an interim update.

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@GORSE.org.uk | **W** www.GORSE.org.uk

GORSE

2. What is a Data-Breach?

2.1 Article 4 of the UK General Data Protection Regulation (GDPR) defines a personal data breach as:

'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 are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data'.

The Information Commissioners Office (ICO) has provided guidance on breaches:

'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.'

(ICO guide to Data-Protection/Guide to the General Data-Protection Requirements (GDPR)/Personal data breaches)

2.2 A data-breach can therefore be summarised as:

- An incident whereby a data-subject's personal data has been shared, amended, lost or deleted without their consent or, if consent is not required, where the legal-basis for processing that data has been breached

2.3 The level of impact or risk arising from a data-breach is driven by key variables:

- Type/sensitivity of the data
- Volume of data
- Level of anonymisation/pseudonymisation within the data
- Volume of third parties involved (in the event of incorrect sharing)

3. Actions for reporting

3.1 In the event that a data-breach is identified there are two clear points of external reporting which may be required:

- Notification to the individuals (data-subjects) involved

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@GORSE.org.uk | **W** www.GORSE.org.uk

- Notification to the ICO

3.2 The rationale for the decision to report is based around the level of risk involved and the likelihood of the breach causing harm to the data-subject(s) – this is a decision based on the 4 variables defined within section 2.

3.3 Within GORSE the accountability for making the decision on whether reporting is necessary, and at which level, has been delegated by the Chief Executive Officer to the Strategic Lead Officer and the Deputy Strategic Lead Officer (The Central Data Governance Team - CDGT). The decision on reporting is made utilising the information provided and, where necessary, through conversation with the GORSE Data-Protection Officer.

3.4 The trust establishment should immediately inform the CDGT of any known breaches, suspected breaches or near-misses. Alongside the requirement to inform the CDGT, any member of staff at the trust establishment should immediately notify the establishment Chief Privacy Officer (CPO) and the Principal/Equivalent. Within Appendix 1 there is a flow diagram which demonstrates the end-to-end process for reporting and managing any data-breach or near-miss:

- The email contact for the CDGT is: datarequests@GORSE.org.uk
- Principals/Equivalents and CPO's also have direct contact details for CDGT team members

3.5 It should be stressed that the timeliness of reporting is of high importance, to ensure:

- That the rights of the data-subject are protected
- That any communication with data-subjects is prompt - to alleviate concern
- That we commence any recovery actions promptly - to mitigate further impact
- That in the event of an ICO reportable breach we achieve 72-hour reporting

3.6 Initial reporting to the CDGT should include details of:

- Type/sensitivity of the data
- Volume of data
- Level of anonymisation/pseudonymisation within the data
- Volume of third parties involved (in the event of incorrect sharing)
- Details of data-subjects involved
- Details of any staff involved
- How the breach/near-miss was identified

3.7 Where necessary the CDGT will request that the trust establishment completes the form shown in Appendix 2.

4. Actions to manage recovery

Following assessment of the breach/near-miss the CDGT will:

- Seek guidance from the GORSE Data-Protection Officer – as necessary
- Inform the GORSE executive – as necessary
- Manage any reporting to the ICO (via the GORSE Data-Protection Officer) – as necessary

And will work with the trust establishment team (and GORSE teams as necessary – e.g. IT) to:

- Identify data-subjects
- Draft, review and approve any communications to data-subjects
- Confirm rectification actions for the data concerned
- Confirm training records of any staff involved
- Confirm any post-event corrective actions required (e.g. additional staff training)

Individual trust establishments should not commence any rectification work, make contact with any data-subjects, contact the GORSE Data-Protection Officer, or contact the ICO directly – until they have liaised with the CDGT.

5. Actions to reduce risk

5.1 GORSE establishments have several tools available to them to help reduce and/or mitigate risk of data-breach or near-miss, these include:

- Ensuring that within each establishment there are the necessary structures, policies and processes in place to manage personal data
- Ensuring that all staff have a full understanding of their own roles and responsibilities through the completion of mandatory training
- Providing regular communication to all staff – to identify risk and the responsibility of all staff to manage this risk
- Completing self-audit on a regular basis – predominantly through the use of the data-walk tool, to identify levels of compliance and risk within their establishment
- Utilising the GORSE Data-Privacy Impact Assessment Policy for any new or amended elements of data processing

5.2 The CDGT will provide trust-level insight to the CPO group, and wider leadership teams, to identify areas of risk and actions for improvement at a trust level.

6. Actions to review and mitigate further instances

6.1 Following any breach or near-miss the CDGT will provide the establishment CPO with any recommendations for improvement, because of the specific case. Where appropriate the team will also bring areas for improvement to the wider CPO group for cascade within the full trust.

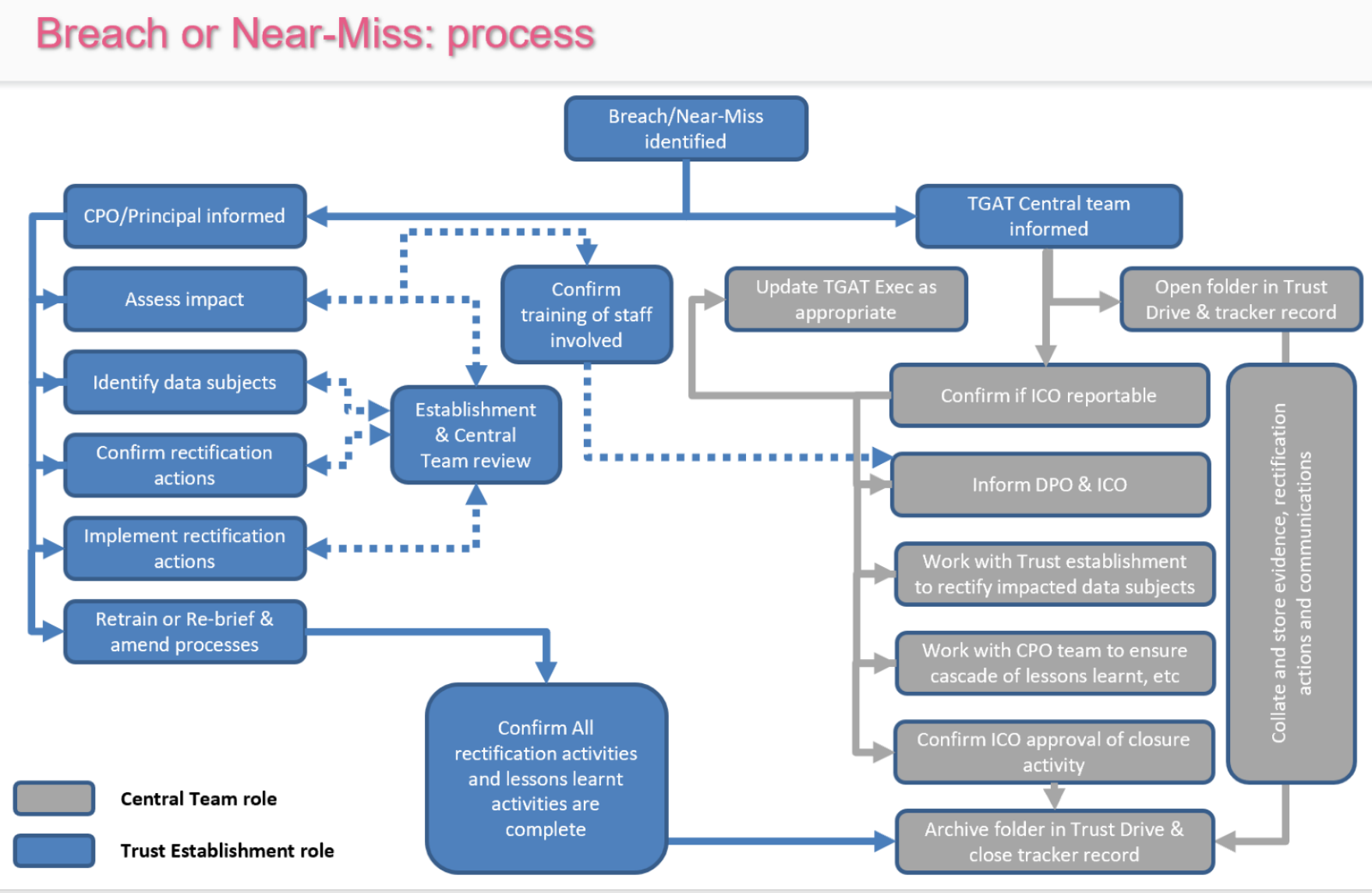
6.2 The CDGT will track patterns and trends within data-breaches and near-misses, for the following reasons:

- To assist in identifying areas of establishment strength and weakness
- To assist in identifying areas of GORSE strength and weakness
- To assist in development of training and communication strategies
- To assist in development of policy
- To enable reporting to:
  - GORSE Data-Protection and Cyber-Security Steering Group: termly
  - GORSE Board (Audit and Risk Committee): annually

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@GORSE.org.uk | **W** www.GORSE.org.uk

GORSE

Appendix 1 – Data-Breach Management process:



GORSE

Appendix 2 – Data-Breach Management Form

Description of the Data Breach (e.g., laptop stolen from vehicle)**:**	
Time and Date the breach occurred (if known).	
Time and Date the breach was discovered, method and by whom.	
Who is reporting the breach: Name/Post/Dept	
Contact details: Telephone/Email	
Categories of personal data included in the breach. Mark ALL categories involved or potentially involved. Very important: If the data involved is in either the Sensitive or Confidential category, then you must forward this report to the school data lead immediately.	**Basic Information** Basic personal identifiers, e.g., name, title Contact information, e.g., telephone, email, address Identification data, e.g., usernames, passwords **Other** (Please specify): **Special Category Data (Sensitive)** Data revealing racial or ethnic origin Health Data (incl. Medical conditions or Mental Health). Political opinions or affiliations Trade Union membership Religious or philosophical beliefs Sex life data Sexual orientation data Gender reassignment data Criminal convictions, offences Genetic or biometric data **Other** (Please specify):

GORSE

	Confidential Data
	Date of Birth (of an adult) ☐
	National Insurance Number ☐
	Official documents e.g., driving licences, passports ☐
	Financial data, e.g., credit card numbers, bank details ☐
	Location data ☐
	Other (Please specify):
Number of personal data records involved.	
Number of data subjects that could be affected.	
(if numbers unknown record the maximum possible number, with final number to be confirmed)	
Categories of data subjects involved. Mark **ALL** categories involved or potentially involved. **Important:** Vulnerable includes SEND, a pupil with safeguarding concern or any individual with, or potentially with, a mental health issue.	Pupil(s) ☐ Ex Pupil(s) ☐ Staff ☐ Ex-Staff ☐ Parent or Guardian ☐ Visitor ☐ Potential Parent or Pupil ☐ Vulnerable Pupil ☐ Vulnerable Adult ☐ **Other** (Please specify):
Confirmed or suspected breach?	Confirmed ☐ Suspected ☐

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@GORSE.org.uk | **W** www.GORSE.org.uk

GORSE

Potential consequences of the breach?	
What is the likely hood that data subjects will experience significant consequences because of the breach?	Very Likely ☐ Likely ☐ Unlikely ☐ Very Unlikely ☐ Not yet known ☐
Reason(s) to support the likely hood selected.	
Is the breach contained or ongoing?	Contained ☐ Ongoing ☐
If ongoing, what actions are being taken to recover the data?	
Who has been informed of the breach?	
Any other relevant information.	

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@GORSE.org.uk | **W** www.GORSE.org.uk

Reason for version change:	Policy Review Cycle	Version number:	1.1
Date of Approval:	June 2024	Approved by:	Policy Committee
Target Audience:	All staff – cascade via Principals CPO Group	Date issued:	June 2024

The GORSE Academies Trust
c/o John Smeaton Academy, Smeaton Approach, Barwick Road, Leeds, LS15 8TA
T 0113 487 8888 | **E**: info@GORSE.org.uk | **W** www.GORSE.org.uk