Plymouth CAST
Multi Academy Trust

Plymouth CAST Data Breach Policy and Procedure

First issue: October 2018

Document Control

Changes History

Version	Date	Amended by	Recipients	Purpose
1.0	Oct 2018	Matthew Barnes Deputy Director of Education and Standards	All Plymouth CAST staff	New GDPR Legislation

Approvals

This policy requires the following approvals:

Board	Chair	CEO	Date Approved	Version	Date for Review
			October 2018	2.0	October 2020

National/Local Policy

☐ This policy must be localised by schools

☐ This policy must not be changed, it is a National Policy (only change logo, contact details and yellow highlighted sections)

Position with the Unions

Does the policy require consultation with the National Unions under our recognition agreement? ☐ Yes ☐ No If yes, the policy status is: ☐ Consulted and Approved ☐ Consulted and Not Approved ☐ Awaiting Consultation

Distribution

This document has been distributed to:

Position	Date	Version
All Plymouth CAST HTs	October 2018	1.0
All Plymouth CAST DSLs	October 2018	1.0
Plymouth CAST Directors and SEL	October 2018	1.0

Contents

Document Control	Page 2
Contents	Page 3
1. Introduction	Page 4
2. Purpose and scope	Page 4
3. Definition / types of breach	Page 4
4. Reporting an incident	Page 5
5. Containment and recovery	Page 5
6. Investigation and risk assessment	Page 5
7. Notification	Page 6
8. Evaluation and response	Page 7
Appendix 1 – DATA BREACH REPORT FORM	Page 8

1. Introduction

1.1 Plymouth CAST and it's schools (for the purposes of this policy, both will be referred to as the Trust) holds, processes and shares a large amount of personal data, a valuable asset that needs to be protected.

1.2 Every care is taken to protect personal data from incidents (either accidental or deliberate) to avoid a data protection breach that could compromise security.

1.3 Compromise of information, confidentiality, integrity, or availability may result in harm to individuals' reputational damage, detrimental effect on service provisions, legislative non-compliance, and/or financial costs.

1.4 This policy sits alongside the Trust's Data Protection Policy and should be read in conjunction with that policy.

2. Purpose and scope

2.1 The Trust is obliged under the Data Protection Act 2018 and the General Data Protection Regulation to have in place a framework designed to ensure security of all personal data during its lifecycle, including clear lines of responsibility.

2.2 This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the Trust.

2.3 This policy relates to all personal and special category data held by the Trust regardless of format.

2.4 This policy applies to all staff, volunteers, stakeholders and contractors at the Trust. This includes leaders, teachers, teaching students, temporary and casual staff, agency staff, and suppliers and data processors working for, or on behalf of, the Trust.

2.5 The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what remedial action is necessary to secure personal data and prevent further breaches.

3. Definition / types of breach

3.1 For the purposes of this policy, data security breaches include both confirmed and suspected incidents.

3.2 An incident in the context of this policy is an event which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately and has caused or has the potential to cause damage to the Trust's information assets and/or reputation.

3.3 An incident includes, but is not restricted to the following:

- Loss or theft of confidential or special category data, or equipment on which such data is stored (e.g. loss of a laptop, memory stick, iPad/Tablet, or paper record);
- Equipment theft or failure;

- Unauthorised use, access, or modification of data or information systems;
- Attempts (failed or successful) to gain unauthorised access to information or IT systems;
- Unauthorised disclosure of special category and confidential data;
- Website defacement;
- Hacking attack;
- Unforeseen circumstances such as a fire or flood;
- Human error;
- Blagging offences where information is obtained by deceiving the organisation who holds it.

4. Reporting an incident

4.1 Any individual who accesses, uses or manages data for the Trust, either centrally or in one of the Trust's schools, is responsible for reporting any data breach and information security incidents immediately to the Data Controller in their school.

4.2 The Data Breach must be recorded on the GDPRiS website. The report must include full and accurate details of the incident, when the breach occurred, details of the person reporting the breach, whether the breach relates to people, the nature of the information, and how many people are involved.

4.3 The Designated Safeguarding Lead (DSL) of the trust will review all data breaches that are logged onto the GDPRiS website with 2 working days of the record being made. They will consider whether the recorded breach is likely to need to be referred to the Information Commissioner's Office (ICO). If the DSL believes the breach is reportable to the ICO, the DSL will complete a Data Breach Report Form (Appendix 1) and email it to the Trust's appointed DPO (Matthew Barnes, Deputy Director of Education and Standards) within 24 hours of reviewing the original record. The DPO will review the Data Breach Report Form and make the final decision to refer the breach to the ICO (Please see notification section below)

4.4 If a breach occurs or is discovered outside normal working hours, it must be reported as soon as practicable. The Trust has only 72 hours to report a breach to the Information Commissioner's Office.

5. Containment and recovery

5.1 Once a notification has been received, the Data Coordinator will determine if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effect of the breach.

5.2 An initial assessment will be made by the Data Coordinator, in liaison with relevant staff, to establish the severity of the breach and who will lead any investigation.

5.3 The Lead Investigation Officer (LIO), who will typically be a Data Coordinator in schools and the DPO for the trust, will establish who may need to be notified as part of the initial containment and will inform the police, if appropriate.

5.4 The LIO, in liaison with relevant staff, will decide upon a suitable course of action to be taken to ensure a resolution to the incident.

6. Investigation and risk assessment

6.1. An investigation will be undertaken by the LIO immediately and where possible within 24 hours of the breach being discovered or reported.

6.2 The LIO will investigate the breach and assess the risks associated with it. For example, the potential adverse effects for individuals, how serious or substantial those are and how likely they are to occur.

6.3 The investigation will need to take into account the following:

- the type of data involved;
- it's sensitivity;
- the protection in place (e.g. encryption);
- what's happened to the data, has it been lost or stolen;
- whether the data could be put to illegal or inappropriate use;
- who the individuals are, the number affected and the potential effects on those data subjects;
- whether there are wider consequences to the breach.

7. Notification

7.1. The DPO will determine whether the breach needs to be reported to the Information Commissioner's Office. Once a decision is made, the DPO will inform the DSL. The DSL will inform the relevant Data Controller if the decision is to refer to the ICO.

7.2 Every incident will be assessed on a case by case basis against the following considerations:

- whether there are any legal or contractual notification requirements;
- whether notification would assist the individual affected – could they act on information to mitigate the risks;
- whether notification would help prevent the unauthorised or unlawful use of personal data;
- would notification help the Academy meet its obligations under the principle;
- whether this breach constitutes a high risk to individuals and therefore needs to be reported to the ICO.

7.3 Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the Trust for further information, or to ask questions about what has occurred.

7.4 The DPO must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

7.5 The DPO will consider whether any press release may be required.

7.6 All actions will be recorded by the DPO using the GDPRiS website.

8. Evaluation and response

8.1. Once any incident that has needed to be referred to the ICO is contained, the DPO will carry out a full review of the causes of the breach, the effectiveness of the response and whether any changes to systems, policies or procedures should be undertaken.

8.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

8.3 The review will consider:

- where and how the personal data is held and where it is stored;
- where the biggest risks lie, and will identify any further potential weak points within its existing measures;
- whether methods of transmission are secure - sharing the minimum amount of data necessary
- identifying weak points within existing security measures;
- staff awareness;
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

Annex 1 – DATA BREACH REPORT FORM – To be completed by trust DSL

If your evaluation of a recorded data breach is that it fits the criteria to refer to the ICO, please complete all sections below. If you are unable to answer any question, please contact the Data Controller at the relevant organisation to get the information needed. Once complete, please send the form to the DPO: matthew.barnes@plymouthcast.org.uk

SECTION 1: Notification of data security breach

Date of incident:	
Date incident was discovered:	
Place of incident:	
Person reporting incident:	
Contact details of person reporting incident:	
Brief description of incident:	
Details of information/data lost or stolen:	
Brief description of any action taken at the time of the discovery:	

For use of DPO:

Received by:	
Date received:	
Forwarded for action to:	
Date forwarded for action:	

SECTION 2: **Assessment of severity** (to be completed by the Lead Investigation Officer (LIO) in consultation with the DSL and DPO, where appropriate)

Details of the IT systems, equipment, devices, and records involved in the security breach:	
Details of the information loss/breach:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost or stolen how recently was this last backed up onto central IT systems?	

Is the information unique? Will its loss have adverse operational, legal, liability, or reputational consequences for the Academy or third parties?	
How many Data Subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into the following categories:	
HIGH RISK personal data. Special Category data (as defined in the Data Protection Act 2018) relating to a living, identifiable individual's@: a) Racial or ethnic origin; b) Political opinions or religious or philosophical beliefs; c) Membership of a trade union; d) Physical or mental health, or condition, or sexual life; e) Biometric data	
Information that could be used to commit identify fraud such as: a) Personal bank account and other financial information; b) National identifiers, such as NI number; c) Copies of passports or visas	
Personal information relating to parents, staff and children	
Detailed profiles of individuals including information about work performance, salaries or personal life that would	

cause significant damage or distress to that person if disclosed	
Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline, or sensitive negotiations which could adversely affect individuals	
Security information that would compromise the safety of individuals if disclosed	

SECTION 3: Action taken (to be completed by the Data Protection Officer (DPO) and / or Lead Investigation Officer (LIO)

Incident number (e.g. year/001):	
Report received by:	
Date report received:	
Action taken by responsible officers:	
Was incident reported to the police (YES/NO)? If notified please record the date:	
Follow up action required/recommended:	

For use of DPO:

Notification to the ICO (YES/NO). If yes, please record detail of notification and date notified:	
Notification to Data Subjects (YES/NO). If yes, please record detail of notification and date notified:	
Notification to other external regulator or stakeholder (YES/NO).	

If yes, please record detail of notification and date notified:	