Dartmoor
MULTI ACADEMY TRUST

Personal Data Breach Procedure

Adopted on the 23 May 2018

To be reviewed May 2021

Document control	
Authorised By	Trustees
Published Location	www.dartmoormat.org
Other documents referenced	
Related documents	

Version control			
Version Number	Date issued	Author	Update information
1.0	23 May 18	DPO	First Published
1.1	18 Oct 18	DPO	Revised edition, simplified for staff, pupil and parent use. Review date amended.

Introduction

Dartmoor Multi Academy Trust holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Dartmoor Multi Academy Trust.

This breach procedure sets out the course of action to be followed by all staff at any school of the Dartmoor Multi Academy Trust if a data protection breach takes place.

The Head Teacher/ Head of School as the Data Controller is responsible for ensuring that staff are aware of the Trust's Data Protection Policy and its requirements including this Breach Procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, Head Teacher or the DPO.

Data Breach Procedure

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO. School staff have access to their school's GDPRis software where a breach can be logged, which will automatically alert the DPO and head teacher.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary as soon as possible.

The DPO will investigate the report, in conjunction with data protection lead staff at the school, and determine whether a breach has occurred, using the Data Breach Assessment Form in Appendix 1. In completing the assessment, the DPO will consider whether personal data has been accidentally or unlawfully lost, stolen, destroyed, altered, disclosed or make available where it should not have been or made available to unauthorised people

The Head Teacher in conjunction with the DPO must also consider whether the Police need to be informed. 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. In such instances, advice from the Trust's legal support should be obtained.

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

The DPO will work out whether the breach is notifiable to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

The DPO will document every breach and decision using the Appendix 1 form.

Completed Data Breach Assesesments will be stored in GDPRis account of the school where the breach occurred

Each assessment will include details of action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Notifiable Breaches

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

Notifying individuals

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

When notifying individuals, we will give specific and clear advice on what they can do to protect themselves and what the trust is able to do to help. We will give them the opportunity to make a formal complaint if they wish (see the Trust's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. We will include details of what we have already done to mitigate the risks posed by the breach

Steps to mitigate data breaches

- Attempting to recover lost equipment.
- Contacting the relevant IT department, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Head Teacher/DPO.

- The use of back-ups to restore lost/damaged/stolen data.
- If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
- If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Actions to minimise the likelihood and impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- Special category data (sensitive information) will be sent by encrypted mail wherever possible.
- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other steps to minimise data breaches should include:

- Staff are actively encouraged to use SharePoint and Google Docs for the secure storage of school information rather than USB sticks. Only where there are restrictions to do so, will data sticks be permitted and they must be encrypted.
- Regular training of all staff is expected of head teachers and their senior staff to ensure that awareness remains high with all staff so that privacy by design and privacy by action can minimise data breach risks.
- Staff are reminded routinely to lock their computer screens when away from their desks.
- Staff are reminded not to include pupil names in email subject headers.
- The use of a shared forum by Data Champions within each school is designed to encourage the sharing of best practice in data management.

Data Breach Assessment Form

School	
Head Teacher	
Breach reported date/time	
DPA completed by	
DPO reviewed date	

1. School to complete the assessment fields.
2. DPO to evaluate scoring with reference to “Recommendations for a methodology of the assessment of severity of personal data breaches” Enisa (European Union Agency for Network and Information Security)

A. Data Processing Context	
Precisely what type of data has been (or is thought to have been) lost, damaged or compromised? What identifiers were used? (first name, full name, address, images, etc.)	
How accurate /current was the data?	
Is any of the data Sensitive Personal Data (see Appendix A)	
Could the data have been publicly available? e.g. information on a website	
How many individuals have definitely been affected and how many potentially affected in a worst case scenario?	
Who are the affected individuals e.g. staff, parents, pupils, third parties?	
Score	

B. Ease of identification How easily can the identity of individuals be deduced from the data involved in the breach, taking into account the context described above and the number and type of different data items? Detail any other considerations.	
1. **Negligible:** e.g. no other information is available to identify the individual/s 2. **Limited:** unclear or vague identifiers 3. **Significant**: data items linked e.g. photo plus name; unique within population e.g. unusual names or details, clear images, primary contact information revealed 4. **Maximum**: clear and readily identifiable from data	
Score	

C. Circumstances of breach

Could harm be caused to individuals (not necessarily those whose personal data was involved in the breach)? Harm should be interpreted broadly as defined in Appendix B.		
Was the breach due to an intentional action in order to harm individuals?		
What harm might be caused to the school or trust? e.g. reputational damage and financial loss		
Detail any physical or technical security measures in place e.g. locked case, encryption.		
Detail any measures taken to *limit* the breach e.g. notifying recipients to delete messages or check security of accounts. Detail measures taken to *recover* lost data.		
Score		

Supplemental Considerations

Please consider the following headings to assist in checking that all issues surrounding the data breach have been considered. It is not an exhaustive list but may assist the panel when assessing the consequences of the data breach.

Pupil/ Staff welfare	
Complaints	
Pupil/ staff disciplinary action	
Pupil/ staff training needs	
Reputation management	
Risks of legal claims	
Possible ICO action	

Severity Assessment **to be completed by DPO**
(A x B + C)

A. Data Processing Context	
B. Ease of identification	
C. Circumstances of breach	
Assessment	

Severity of a data breach		
SE < 2	**Low**	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	**Medium**	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE< 4	**High**	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ SE	**Very High**	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

Appendix A: Sensitive data

a) information concerning child protection matters;
b) information about serious or confidential medical conditions and information about special educational needs;
c) information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);
d) financial information (for example about parents and staff);
e) information about an individual's racial or ethnic origin; and
f) political opinions;
g) religious beliefs or other beliefs of a similar nature;
h) trade union membership;
i) physical or mental health or condition;
j) genetic information;
k) sexual life;
l) information relating to actual or alleged criminal activity; and
m) biometric information (e.g. a pupil's fingerprints following a criminal investigation).

If any of these types of data are involved this makes the breach more serious.

Appendix B: Harm

Harm may be interpreted as:
a) distress;
b) discrimination;
c) loss of confidentiality;
d) financial damage;
e) identity theft;
f) physical harm;
g) reputational damage
h) loss of integrity of data (such as could cause harm to the individual)