THIS POLICY COVERS ALL ACADEMIES/SCHOOLS WITHIN ARDEN MULTI-ACADEMY TRUST

Name of Policy	**Data Breach Procedure**	
Lead	Martin Murphy, CEO	
Governor Committee	Business & Personnel Committee	
Policy Status	Taken from Browne Jacobson Policy	November 2025
	Trustee Approved	09/12/2025
Next Review	Autumn Term 2026	
Version No.	1	
Amendments		

Personal Data Breach Procedure

Statement

1 Arden Multi-Academy Trust (Arden MAT) is committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller** as set out in our Data Protection Policy.

2 All members of our **workforce** must comply with this procedure when becoming aware of a **personal data** breach. Any breach of this procedure may result in disciplinary or other action.

About this procedure

3 This procedure informs all of our **workforce** on how to respond when dealing with a suspected or identified **personal data breach**.

4 In the event of a suspected or identified breach, Arden MAT must take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring.

5 Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible.

6 The Arden MAT must also comply with its legal and contractual requirements to notify other organisations including the **Information Commissioner's Office** ("the **ICO**"), the National Cyber Security Centre ("**NCSC**"), or Action Fraud and where appropriate **data subjects** whose **personal data** has been affected by the breach. This includes any communications with the press.

7 Failing to appropriately deal with and report data breaches can have serious consequences for the Arden MAT and for **data subjects** including:

7.1 identity fraud, financial loss, distress or physical harm;

7.2 reputational damage to Arden MAT; and

7.3 regulatory sanction from the **ICO**.

Definition of data protection terms

8 All defined terms in this procedure are indicated in bold text, and a list of definitions is included in Annex 2 to this procedure.

Identifying a personal data breach

9 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**.

10 This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A

data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches are listed below:

10.1 Leaving a mobile device on a train;

10.2 Theft of a bag containing paper documents;

10.3 Destruction of the only copy of a document; and

10.4 Sending an email or attachment to the wrong recipient; and

10.5 Using an unauthorised email address to access personal data; and

10.6 Leaving paper documents containing personal data in a place accessible to other people.

Internal communication

Reporting a personal data breach upon discovery

11 If any member of our **workforce** suspects, or becomes aware, that a **personal data breach** may have occurred (either by them, another member of our **workforce**, a **data processor**, or any other individual) then they must [contact the Data Protection Officer ("the **DPO**")] immediately at: gjdavies@lodeheath.org.uk.

12 The data breach may need to be reported to the **ICO**, and other bodies such as the NCSC and Action Fraud and notified to **data subjects**. This will depend on the risk to **data subjects**. The DPO must always be consulted in making a decision as to whether to report a data breach to the **ICO**. Initial investigations will inform whether and to whom the data breach should be reported to external bodies and/or **data subjects**.

13 Where there is a risk to **data subjects**, the data breach must be reported to the **ICO** within 72 hours of discovery of the breach. If it is not possible to report within 72 hours, notification must still take place, but should be accompanied by the reasons for the delay in reporting.

14 Where there is a high risk to **data subjects**, then the data breach must be reported to those individuals without undue delay.

15 Where there is a cyber related incident which involves an attacker gaining access to IT systems then the NCSC must be informed. The NCSC is not a law enforcement or regulatory body so will not treat incidents reported as a crime. If a crime has taken place, then this should be reported to Action Fraud.

16 The Arden MAT may also be contractually required to notify other organisations of the breach within a period following discovery.

17 It is therefore critically important that whenever a member of our **workforce** suspects that a data breach has occurred, this is reported internally to the DPO immediately.

18 Members of our **workforce** who fail to report a suspected data breach could face disciplinary or other action.

Investigating a suspected data breach

19 In relation to any suspected data breach the following steps must be taken as soon as possible. These do not have to be carried out as individual tasks, and the most appropriate way of dealing with any breach will depend on the nature of the breach and the information available at any time.

Breach minimisation:

20 The first step must always be to identify how the data breach occurred, the extent of the data breach, and how this can be minimised. The focus will be on containing any data breach and recovering any **personal data**. Relevant departments and staff may be involved, such as IT personnel or parent liaison staff, to take technical and practical steps where appropriate to minimise the breach. Appropriate measures may include:

20.1 remote deactivation of mobile devices;

20.2 shutting down IT systems;

20.3 contacting individuals to whom the information has been disclosed and asking them to delete the information; and

20.4 recovering lost data.

Breach investigation:

21 When the Arden MAT has taken appropriate steps to minimise the extent of the data breach it must commence an investigation as soon as possible to understand how and why the data breach occurred. This is critical to ensuring that a similar data breach does not occur again and to enable steps to be taken to prevent this from occurring.

22 Technical steps are likely to include investigating, using IT forensics where appropriate, to examine processes, networks and systems to discover:

22.1 what data/systems were accessed;

22.2 how the access occurred;

22.3 how to fix vulnerabilities in the compromised processes or systems;

22.4 how to address failings in controls or processes.

23 Other steps are likely to include discussing the matter with individuals involved to appreciate exactly what occurred and why, and reviewing policies and procedures.

24 Where the DPO is unsure how to mitigate the breach, or what steps to take, they will call the **ICO** helpline on 0303 123 1113 for assistance

Breach analysis:

25 In order to determine the seriousness of a data breach and its potential impact on **data subjects**, and so as to inform the Arden MAT as to whether the data breach should be reported to the **ICO** and notified to **data subjects**, it is necessary to analyse the nature of the data breach.

26 Such an analysis must include:

26.1 the type and volume of **personal data** which was involved in the data breach;

26.2 whether any **special category personal data** was involved;

26.3 the likelihood of the **personal data** being accessed by unauthorised third parties;

26.4 the security in place in relation to the **personal data**, including whether it was encrypted;

26.5 the risks of damage or distress to the **data subject**.

27 The **ICO** breach notification form annexed to this procedure provides a useful prompt for the questions that should be considered when reporting every case of a suspected breach, whether or not a decision is ultimately made to report the data breach to the **ICO**. This will ensure sufficient information is gathered at the earliest opportunity as well as acting as evidence as to the considerations of the Arden MAT in deciding whether or not to report the breach as well and forming the basis of a prompt notification to **ICO** within statutory requirements.

External communication

28 All external communication is to be managed and overseen by the DPO, the relevant Associate Headteacher or AMAT CEO.

Law Enforcement

29 The DPO and/or associate headteacher or CEO will assess whether the data breach incident requires reporting to any law enforcement agency, including the police. This will be informed by the investigation and analysis of the data breach, as set out above.

30 DPO and/or associate headteacher or CEO shall coordinate communications with any law enforcement agency.

Cyber Security

31 Where a cyber incident has taken place, an assessment as to whether the incident is required to be reported to appropriate advice and law enforcement agencies must take place. The DPO and/or associate headteacher or CEO must complete the assessment tool at https://www.gov.uk/guidance/where-to-report-a-cyber-incident which indicates whether reporting is required, and if so, to which agencies, including NCSC or Action Fraud. If such reporting is required, then the DPO and/or associate headteacher or CEO will be responsible for this reporting, using the contact details for the relevant agencies given at the end of the assessment process.

Other organisations

32 If the data breach involves **personal data** which we process on behalf of or as **joint controller** with other organisations, then we may be contractually required to notify them of the data breach.

33 The Arden MAT will identify as part of its investigation of the data breach whether or not this is the case and any steps that must be taken as a result.

Information Commissioner's Office

34 If Arden MAT is the **data controller** in relation to the **personal data** involved in the data breach, which will be the position in most cases, then the Arden MAT has 72 hours to notify the **ICO** if the data breach is determined to be notifiable.

35 A data breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of any individual. The DPO will make an assessment of the data breach against the following criteria taking into account the facts and circumstances in each instance:

35.1 the type and volume of **personal data** which was involved in the data breach;

35.2 whether any special category personal data was involved;

35.3 the likelihood of the **personal data** being accessed by unauthorised third parties;

35.4 the security in place in relation to the **personal data**, including whether it was encrypted;

35.5 the risks of damage or distress to the **data subject**.

36 If a notification to the **ICO** is required then see part 35 of this procedure below.

37 Where the DPO is unsure whether the data breach meets the threshold to report, they will call the **ICO** helpline on 0303 123 1113 for assistance.

38 In the vast majority of cases the Arden MAT will be acting as **data controller**, however if the Arden MAT is ever acting only as **data processor** then on identifying any breach it should only report the matter to the organisation which is the **data controller**, whose responsibility it is to then investigate the breach, though cooperation may be required from the Arden MAT.

Other supervisory authorities

39 If the data breach occurred in another country or involves data relating to **data subjects** from different countries, then the [DPO] will assess whether notification is required to be made to supervisory authorities in those countries.

Data subjects

40 When the data breach is likely to result in a high risk to the rights and freedoms of the **data subjects** then the **individuals affected** must be notified without undue delay. This will be informed by the investigation of the breach by the Arden MAT.

41 The communication will be coordinated by the DPO and/or associate headteacher or CEO and will include at least the following information:

41.1 a description in clear and plain language of the nature of the data breach;

41.2 the name and contact details of the DPO;

41.3 the likely consequences of the data breach;

41.4 the measures taken or proposed to be taken by Arden MAT to address the data breach including, where appropriate, measures to mitigate its possible adverse effects;

41.5 if relevant, advice to affected data subjects about how they may seek further advice and support from an appropriate support organisation (e.g. from the NCSC)

42 There is no legal requirement to notify any individual if any of the following conditions are met:

42.1 appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach, in particular, measures which render the data unintelligible to unauthorised persons (e.g. encryption);

42.2 measures have been taken following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;

42.3 it would involve disproportionate effort to contact individuals. In which case a public communication or similar equally effective measure of communication to the data subjects shall be issued.

43 For any data breach, the **ICO** may mandate that communication is issued to **data subjects**, in which case such communication must be issued.

Insurance

44 Depending on the severity and nature of the data breach it may be necessary to inform the Arden MAT insurance provider [set out details here for contact details for the insurance provider]

Press

45 Staff shall not communicate directly with the press and shall treat all potential data breaches as confidential unless otherwise instructed in writing by the DPO.

46 All press enquiries shall be directed to the Arden MAT CEO via amat@arden.solihull.sch.uk.

Producing an ICO Breach Notification Report

47 All members of our **workforce** are responsible for sharing all information relating to a data breach with the DPO, which will enable the annexed Breach Notification Report Form to be completed when reporting to the **ICO**.

48 When completing the attached Breach Notification Report Form all mandatory (*) fields must completed, and as much detail as possible should be provided.

49 The DPO may require individuals involved in relation to a data breach to each complete relevant parts of the Breach Notification Form as part of the investigation into the data breach.

50 If any member of our **workforce** is unable to provide information when requested by the DPO then this should be clearly reflected in the Breach Notification Form together with an indication as to if and when such information may be available.

51 In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

52 The **ICO** requires that the Arden MAT completes standard online form when reporting to them. Breach reports should be submitted online at https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/report-a-data-breach-online-form/ The Breach Notification Report at the Annex contains the questions for which the answers will need to be copied into the online form to submit the notification.

Evaluation and response

53 Reporting is not the final step in relation to a data breach. The Arden MAT will seek to learn from any data breach.

54 Therefore, following any breach an analysis will be conducted as to any steps that are required to prevent a breach occurring again. This might involve a step as simple as emailing all relevant members of our **workforce** to reinforce good practice, or providing additional training, or may in more serious cases require new technical systems and processes and procedures to be put in place.

Review

55 This procedure is reviewed every 2 years by the Data Protection Officer.

56 The next scheduled review date for this procedure is Spring 2028.

Annex 1 – ICO Breach Notification Report

[To be used if access cannot be gained to GDPRiS]

Tick this box to confirm: I am authorised to report this breach on behalf of my organisation.	☐
Why are you reporting the breach to the ICO?	
When did the breach happen?	
When did you find out about the breach?	
Please enter a time.	
Are you reporting the breach within 72 hours of finding out about it?	
Why were you delayed in reporting the breach?	
How did the organisation find out the breach had happened?	
What happened?	
Was the breach caused by a cyber security attack?	
How did the breach happen?	
Are you able to identify staff members involved in this breach?	
Had the members of staff received data protection training in the two years prior to the breach?	
What was the training they received?	
What personal data is involved in the breach?	
What categories of personal data were included in the breach? Tick all that apply.	
What categories of people were affected by the breach? Tick all that apply.	
Give details of the other categories of people.	
How many people could be affected?	

How many personal data records have been affected?	
What was, or could be the harm to individuals?	
Is the personal data breach likely to result in a high risk to data subjects?	
Have you told the people affected about the breach?	
What preventative measures did you have in place at the time of the breach?	
How confident are you that you can manage the effects of the breach and stop it happening again?	
What steps have you taken to contain the breach and limit its impact?	
What steps have you, or will you take to stop a similar breach happening in the future?	
Have you, or are you going to report the breach to any other organisations?	
What is your organisation's name?	
What is your organisation's registered address?	
Are you registered with the ICO?	
What is your ICO registration number?	
What is the size of your organisation?	
What is your organisation's sector?	
Is your organisation involved with or signed up to a data protection code of conduct or certification scheme approved by the ICO?	
What is your name?	
What is your email address?	
What is your phone number?	
Is there a best day or time to contact you?	

Is there anything else you want to add?	

Annex 2 – Definitions

Term	Definition
Cyber Incident	Cyber incidents can take many forms, such as denial of service, malware, ransomware or phishing attacks. The RPA state that a cyber incident is "any actual or suspected unauthorised access to any computer, other computing and electronic equipment linked to computer hardware, electronic data processing equipment, microchips or computer installation that processes, stores, transmits, retrieves or receives data". Types of activities that are commonly recognised as being a cyber incident are: • breaches of a system's security policy that affects its integrity or availability • attempts to gain unauthorised access to a system or to data • changes to a system's firmware, software or hardware without the system owner's consent malicious disruption or denial of service.
Data	Information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this procedure include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Joint Controller	Where two or more controllers jointly determine the purposes and means of processing the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes.
Personal Data	Any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to

Term	Definition
	one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controller	The organisation which determines the purposes for which, and the manner in which, any personal data is processed.
Data Processors	Any person or organisation that is not a part of our organisation that processes personal data on our behalf and only on our instructions.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.
Processing	Any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Workforce	Includes, any individual employed by [School/Trust/Academy] such as staff and those who volunteer in any capacity including Governors [and/or Trustees / Members/ parent helpers]