DIOCESE OF WORCESTER MULTI ACADEMY TRUST

TO LOVE | TO LEARN | TO SERVE

DATA BREACH NOTIFICATION POLICY

2021-2023

MAT Board Approval:	December 2019
Last Review:	October 2021
Next Review:	Autumn 2023
Member of Staff Responsible:	Mrs Claire Roberts

Our Vision

'To Love, To Learn, To Serve' sums up the DoWMAT's vision for those who come together to create the MAT, enabling all to flourish both as individuals and in community with each other; living life in all its fullness (John 10:10).

Our Values

To Love

The New Testament sums up the entire law as a call to "love your neighbour as yourself" (Galatians 5:14). The Bible teaches that we are only able to love because God first loved us (1 John 4:10). This love is expected to characterise the way in which the DoWMAT operates, makes decisions, builds relationships, and carries out its day-to-day business: each person putting the needs of others before their own, with a commitment to the flourishing of all. The exposition of love in 1 Corinthians 13 reminds us that love is patient, kind, forgiving, generous, humble, trusting, respectful, hopeful, resilient and enduring. Those who learn and work in the DoWMAT, and all who come into contact with it, can expect to experience that love in the way that they are treated.

To Learn

The DoWMAT is a Christian learning community that is committed to enabling all to live a life of freedom and transformation as a result of the hope and wisdom that learning brings. Learning is at the heart of the Church of England's vision for and commitment to education. Growing in wisdom is celebrated in the Bible and all are exhorted to listen, to seek guidance, to acquire knowledge and to learn discretion (Proverbs 1: 1-6), largely through human relationships and interactions. Jesus' teaching, as summed up in the Beatitudes (Matthew 5:3-10), describes human beings who are learning to live a life that is characterised by humility, compassion, mercy, righteousness and peace. The learning that takes place within the DoWMAT is expected to be recognisably rooted in these godly characteristics and focused upon enabling the holistic development of people who are made in the image of God.

To Serve

Service and servant leadership, was a striking feature of the way in which Jesus lived his life. The example he gave to his disciples in washing their feet (John 13:1-17) provides us with a role model for the way in which we should seek to live in community with others. Putting the needs of others before our own, supporting people in their growth and development as holistic human beings, enabling people's gifts and talents to come to the fore as a result of our service to them are all defining characteristics of the way in which the DoWMAT operates. In serving others and meeting their needs through generosity of spirit, we manifest God's grace and love for others (1 Peter 4:8-11).

These core values underpin all aspects of our Trust as we strive to make a positive difference to the lives of all DoWMAT pupils whilst they are at school and in later life. Through these values, we can be sure our community is one of hope; a place of transformation and trust, where all are treated with respect and dignity.

OUTSTANDING PROFESSIONALS | COLLABORATIVE PARTNERSHIPS | STRONG SYSTEMS | CONFIDENT LEARNERS

1. POLICY STATEMENT

1.1. The Diocese of Worcester Multi Academy Trust (DoWMAT) is committed to the protection of all personal data and special category personal data for which we are the data controller.

1.2. The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

1.3. All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

2. ABOUT THIS POLICY

2.1. This policy informs all of our **workforce** on dealing with a suspected or identified data security breach.

2.2. In the event of a suspected or identified breach, the Trust / Academy must take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring.

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

2.4. The Trust / Academy must also comply with its legal and contractual requirements to notify other organisations including the Information Commissioners Office ("the ICO") and where appropriate **data subjects** whose **personal data** has been affected by the breach. This includes any communications with the press.

2.5. Failing to appropriately deal with and report data breaches can have serious consequences for the Trust / Academy and for **data subjects** including:

2.5.1. Identity fraud, financial loss, distress or physical harm;
2.5.2. Reputational damage to Trust / Academy; and
2.5.3. Fines imposed by the ICO.

3. DEFINITION OF DATA PROTECTION TERMS

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

4. IDENTIFYING A DATA BREACH

4.1. A data breach is a **breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **personal data**.

4.2. 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:

4.2.1. Leaving a mobile device on a train;
4.2.2. Theft of a bag containing paper documents;
4.2.3. Destruction of the only copy of a document; and
4.2.4. Sending an email or attachment to the wrong recipient; and
4.2.5. Using an unauthorised email address to access personal data; and
4.2.6. Leaving paper documents containing personal data in a place accessible to other people.

5. INTERNAL COMMUNICATION

Reporting a Data Breach Upon Discovery

5.1. If any member of our **workforce** suspects, or becomes aware, that a 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:

Mrs Claire Roberts
Field House
29, Sansome Walk
Worcester
WR1 1NU

5.2. The data breach may need to be reported to the ICO, 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 as to whether the data breach should be reported.

5.3. If it is considered to be necessary to report a data breach to the ICO then the Trust / Academy must do so within 72 hours of discovery of the breach.

5.4. The Trust / Academy may also be contractually required to notify other organisations of the breach within a period following discovery.

5.5. 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.

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

(Reporting a breach to the DPO is the minimum that should be required. In addition to a potential data breach being reported to the DPO the Trust / Academy may also consider it appropriate for the matter to be reported to others who will need to be involved in the decision as to whether a data breach should be reported and how best to deal with it. It may be that the Headteacher and the DPO should be notified at the same time so that these individuals can then decide who to involve in the data breach process and to ensure the issue is dealt with effectively and efficiently).

Investigating a Suspected Data Breach

5.7. 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

5.8. 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 must be involved, such as IT, to take technical and practical steps where appropriate to minimise the breach. Appropriate measures may include:

5.8.1. Remote deactivation of mobile devices;
5.8.2. Shutting down IT systems;
5.8.3. Contacting individuals to whom the information has been disclosed and asking them to delete the information; and
5.8.4. Recovering lost data.

Breach Investigation

5.9. When the Trust / Academy 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.

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

5.10.1. That data/systems were accessed;
5.10.2. How the access occurred;
5.10.3. How to fix vulnerabilities in the compromised processes or systems;

5.10.4. How to address failings in controls or processes.

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

Breach Analysis

5.12. In order to determine the seriousness of a data breach and its potential impact on **data subjects**, and so as to inform the Trust / Academy 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.

5.13. Such an analysis must include:

5.13.1. The type and volume of **personal data** which was involved in the data breach;
5.13.2. Whether any **special category personal data** was involved;
5.13.3. The likelihood of the **personal data** being accessed by unauthorised third parties;
5.13.4. The security in place in relation to the **personal data**, including whether it was encrypted;
5.13.5. The risks of damage or distress to the **data subject**.

5.14. The breach notification form annexed to this policy must be completed in every case of a suspected breach, and retained securely, whether or not a decision is ultimately made to report the data breach. This will act as evidence as to the considerations of the Trust / Academy in deciding whether or not to report the breach.

6. EXTERNAL COMMUNICATION

6.1. All external communication is to be managed and overseen by the DPO and the Headteacher.

Law Enforcement

6.2. The DPO and the Headteacher 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.

6.3. The DPO and/or Headteacher shall coordinate communications with any law enforcement agency.

Other Organisations

6.4. If the data breach involves **personal data** which we process on behalf of other organisation's, then we may be contractually required to notify them of the data breach.

6.5. The Trust / Academy 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

6.6. If the Trust / Academy 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 Trust / Academy has 72 hours to notify the ICO if the data breach is determined to be notifiable.

6.7. 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:

6.7.1. The type and volume of **personal data** which was involved in the data breach;
6.7.2. Whether any **special category personal data** was involved;
6.7.3. The likelihood of the **personal data** being accessed by unauthorised third parties;
6.7.4. The security in place in relation to the **personal data**, including whether it was encrypted;
6.7.5. The risks of damage or distress to the **data subject**.

6.8. If a notification to the ICO is required, then see part 7 of this policy below.

Other Supervisory Authorities

6.9. 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

6.10. When the data breach is likely to result in a high risk to the rights and freedoms of the **data subjects** then the **data subject** must be notified without undue delay. This will be informed by the investigation of the breach by the Trust / Academy.

6.11. The communication will be coordinated by the DPO and will include at least the following information:

6.11.1. A description in clear and plain language of the nature of the data breach;
6.11.2. The name and contact details of the DPO;
6.11.3. The likely consequences of the data breach;
6.11.4. The measures taken or proposed to be taken by Trust / Academy to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

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

6.12.1. 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);

6.12.2. 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;

6.12.3. 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.

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

Press

6.14. 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.

6.15. All press enquiries shall be directed to Mrs Claire Roberts, DPO.

7. PRODUCING AN ICO BREACH NOTIFICATION REPORT

7.1. 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.

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

7.3. 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.

7.4. 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.

7.5. 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.

7.6. The ICO requires that the Trust / Academy send the completed Breach Notification Form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

8. EVALUATION AND RESPONSE

8.1. Reporting is not the final step in relation to a data breach. The Trust / Academy will seek to learn from any data breach.

8.2. 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.

ANNEX 1 – ICO Breach Notification Report

1. Organisation Details

Name of Organisation	
Data controller's registration number (if applicable).	
DPO	
Contact Details	

2. Details of The Data Protection Breach

Set out the details of the breach and ensure that all mandatory (*) fields are completed.

(a) * Please describe the incident in as much detail as possible.

(b) * When did the incident happen?

(c) * How did the incident happen?

(d) If there has been a delay in reporting the incident to the ICO please explain your reasons for this.

(e) What measures did the organisation have in place to prevent an incident of this nature occurring?

(f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

3. Details of The Personal Data Placed at Risk

Set out the details of the personal data placed at risk as a result of the breach and ensure that all mandatory (*) fields are completed.

(a) * What personal data has been placed at risk? Please specify if any financial or special category (sensitive) personal data has been affected and provide details of the extent.

(b) * How many individuals have been affected?

(c) * Are the affected individuals aware that the incident has occurred?

(d) * What are the potential consequences and adverse effects on those individuals?

(e) Have any affected individuals complained to the Academy / Trust about the incident?

4. Containment and Recovery

Set out the details of any steps the Academy / Trust has taken to contain the breach and/or to recover the personal data and ensure that all mandatory (*) fields are completed.

(a) * Has the Trust / Academy taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

(b) * Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

(c) What steps has the Trust / Academy taken to prevent a recurrence of this incident?

5. Training and Guidance

Set out the details of any steps the Trust / Academy has taken to contain the breach and/or to recover the personal data and ensure that all mandatory (*) fields are completed.

(a) As the data controller, does the Trust / Academy provide its staff with training on the requirements of Data Protection Legislation? If so, please provide any extracts relevant to this incident here.

(b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

(c) As the data controller, does the Trust / Academy provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

6. Previous Contact with the ICO

(a) * Have you reported any previous incidents to the ICO in the last two years?

YES / NO

(b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. Miscellaneous

(a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.

(b) Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.

(c) Have you informed any other regulatory bodies about this incident? If so, please provide details.

(d) Has there been any media coverage of the incident? If so, please provide details of this.

This form was completed on behalf of the Trust / Academy by:

Name:……

Role:……

Date and Time:……

ANNEX 2 – DEFINITIONS

Term	Definition
Data	Is information which is stored electronically, on a computer, or in certain paper-based filing systems.
Data Subjects	For the purpose of this policy 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.
Personal Data	Means 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controllers	Are the organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data Users	Are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Data Processors	Includes any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Processing	Is 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	Includes 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 Trust / Academy such as staff and those who volunteer in any capacity including Governors and/or Trustees / Members/ parent helpers etc.

Ref: CRo/Sept-21