DIOCESE OF WORCESTER MULTI ACADEMY TRUST

TO LOVE | TO LEARN | TO SERVE

DATA BREACH PROCEDURE

2025-2027

MAT Board Approval:	October 2025
Last Review:	October 2025
Next Review:	Autumn 2027
Member of Staff Responsible:	CEO/DoE

DoWMAT Vision and Values

Our Vision

DOWMAT's vision is to foster an inclusive, nurturing environment where everyone flourishes - academically, spiritually, and personally. Rooted in Christian values, we prioritise the vulnerable, promote work-life balance, and strive to deliver exceptional education, while celebrating each academy's unique identity—reflecting the fullness of life promised in John 10:10.

'To love, to learn, to serve - through collaboration, honesty, and hope.'

Our Values

Love

We are committed to **Compassion and Care**: As Christ commands, we strive to love one another deeply, fostering empathy, respect, and kindness. We create a culture where we genuinely care for each other, supporting personal, professional and spiritual growth, as we walk in His love.

Learn

We are committed to **Continuous Growth and Wisdom**: Following the call to grow in knowledge and understanding, we cultivate a culture of curiosity, adaptability, and continual improvement. We encourage all to seek wisdom and learning, guided by God's truth, that we might serve more effectively.

Serve

We are committed to **Service and Impact**: Inspired by Christ's example of humble service, we dedicate ourselves to serving others, contributing to the well-being of our schools, communities, and beyond, bringing His light and love into all we do.

Collaboration

We are committed to **Unity in Purpose**: We value working together in mutual respect, knowing that through collaboration, we can have a greater impact supporting each other to achieve our shared vision.

Honesty

We are committed to **Integrity and Truth**: Following Christ's call to live in truth, we foster a culture of honesty, transparency, and trust, ensuring that our actions reflect His integrity in all dealings, upholding the highest ethical standards.

Hope

We are committed to **Inspiring Hope and Faith**: As bearers of Christ's hope, we instil in every individual the belief in their God-given potential to achieve great things, trusting in His plan to bring good out of all circumstances, and inspiring hope for a future filled with His promises.

1. Procedure Statement

1.1 The Diocese of Worcester Multi Academy Trust – DoWMAT, ("the Trust" / "we" / "us") processes a significant amount of personal information about its pupils, parents, staff, volunteers and other individuals that it comes into contact with. This can include sensitive information ("Special Category Data").

1.2 By complying with our own internal data protection procedures, and through promoting a strong culture of data protection compliance, our aim is to avoid the occurrence of a data breach. However, we recognise that in the event of a data breach, it is critical that we have effective response procedures in place to minimise the impact on those affected.

1.3 The UK General Data Protection Regulation (the retained EU law version of the General Data Protection Regulation (EU) 2016/679) ("GDPR") places reporting obligations on the Trust, as a data controller, in the event of a data breach. This procedure ("Procedure") has been implemented to ensure that appropriate action is taken in a timely manner to comply with the requirements of the GDPR.

1.4 The Procedure applies to all Trust staff, trustees, volunteers and contractors.

1.5 The Procedure will be reviewed and updated in accordance with documented review dates, though the Trust reserves the right to update this Procedure at any time where it is more immediately necessary to do so e.g. because of operational changes, court or regulatory decisions, or changes in regulatory guidance.

2. Identifying a Data Breach

2.1 A data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. It is therefore important to recognise that a data breach is not just the loss of personal information. Staff are referred to the HYin5ive data protection series for a refresher on what constitutes a data breach (https://hyeducation.co.uk/blog/)

2.2 Examples of data breaches include the following:-

2.1.1 Loss or theft of personal data and / or equipment on which personal data is stored.

2.1.2 Sending personal information to the incorrect recipient.

2.1.3 Unauthorised access of personal information.

2.1.4 Hacking.

2.1.5 Cyber-attack.

2.1.6 Accidental destruction.

2.3 The above list is not exhaustive. If you are in any doubt as to whether a data breach has occurred or not, you should err on the side of caution and report it in accordance with this procedure.

3. Reporting the Breach and Immediate Steps

3.1 Any person at school level who has personally caused a data breach, discovers a data breach, or is informed of the occurrence of a data breach must notify the school's nominated data protection lead, the Headteacher, who must immediately notify the Central Team which can be done by email at Dataprotection@dowmat.education and copying in the CEO. The reported breach will be triaged by the Headteacher and the central team, and if the breach is confirmed as a data breach, this will be immediately reported by the Headteacher to the DPO by telephone (0161 543 8884) or email (DPO@wearehy.com) copying in the central team at Dataprotection@dowmat.education. For all other Trust staff, they should report the breach to the CEO personally by email at Dataprotection@dowmat.education. If the nominated data protection lead is unavailable, school level staff should report the breach to the most senior member of staff on site whom should seek advice from the central team.

3.2 The DPO will be responsible for assessing the data breach and advising the Trust on any immediate action that it may need to take to address any risks arising.

4. Investigation

4.1 The DPO will work with the Trust to investigate the data breach reported, taking such steps as are reasonable to establish the following:-

4.1.1 When the breach occurred.

4.1.2 The factual background.

4.1.3 Who has been affected by the breach e.g. staff, parents and/or pupils.

4.1.4 The number of people affected by the breach.

4.1.5 The type and sensitivity of the personal data concerned.

4.1.6 The consequences or potential consequences of the breach.

4.1.7 The measures taken to minimise the breach.

4.2 The investigation should be completed urgently as its findings will inform whether the Information Commissioner's Office ("ICO") and/or data subjects need to be informed. Where an investigation may take some time, the DPO will consider whether a notification should be made to the ICO notwithstanding the fact that investigations are ongoing.

5. Record of Breach

The DPO must record the data breach in the Data Breach Record.

6. Notification of a Data Breach to the ICO

6.1 Subject to 6.3, and providing the Trust notifies the DPO in a timely manner, the DPO will ensure that a data breach is reported to the ICO not later than 72 hours after the Trust became aware of the breach using the letter template at **appendix 1** for this purpose.

6.2 Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.

6.3 If the data breach is unlikely to result in a risk to the rights and freedoms of those affected by the breach, then the notification to the ICO described at 6.1 will not be necessary.

6.4 A data breach is likely to result in a risk to the rights and freedoms of those affected by the breach if it causes a loss of control over their personal information or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality. These examples are not exhaustive, and the breach must be assessed on a case-by-case basis by the DPO.

6.5 If a notification to the ICO is made, the DPO will ensure that appropriate steps are taken to fully co-operate with their requests / investigations.

7. Notifying the Data Subject(s)

7.1 Subject to 7.2, if the data breach is likely to result in a high risk to the rights and freedoms of data subject(s), the DPO will ensure that steps are taken by the Trust to notify them without delay using the letter template at **appendix 2**.

7.2 Those affected by the data breach need not be notified if any of the following apply:-

7.2.1 the Trust had implemented appropriate technical and organisational measures, and those measures were applied to the personal information affected by the data breach, in particular, those that ensure the personal information is unintelligible to any person who is not authorised to access it, such as encryption and the data is recoverable e.g. as it was backed-up.

7.2.2 the Trust has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.

8. Post Breach Procedure

8.1 It is imperative that regardless of how serious or minor the breach, lessons are learnt, and measures are put in place to avoid a similar incident occurring again in the future. The DPO will be responsible for making any necessary recommendations to improve data protection practices.

8.2 The measures put in place should be proportionate to the breach; however, such measures could include the provision of further training, introduction of new policies and procedures or changes to security measures.

APPENDIX 1

The Information Commissioner's Office

[Insert Address 1]

[Insert Address 2]

[Insert Postcode]

[Date]

Dear Sirs,

Notification of a Data Breach in accordance with Article 33 of the General Data Protection Regulation ("GDPR")

We write to the Information Commissioner's Office in accordance with Article 33 of the GDPR to provide notification of a data breach. It is considered that the breach is notifiable on the basis that it is likely to result in a risk to the rights and freedoms of those affected.

[We are aware that notification should be made to the ICO by no later than 72 hours after having become aware of the data breach. Unfortunately, we were unable to comply with this requirement for the following reasons [XXXXXX]

The nature of the data breach, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned

[INSERT DETAIL]

Name and contact details of the DPO

HY Education Solicitors
Sandbrook House, Sandbrook Way Rochdale
OL11 1RY
DPO@wearehy.com

The likely consequences of the data breach

[INSERT DETAIL]

Measures taken or proposed to be taken by the Trust to address the data breach

[INSERT DETAIL]

We look forward to your office contacting us shortly.

Yours faithfully

APPENDIX 2

[Name]

[Insert Address 1]

[Insert Address 2]

[Insert Postcode]

[Date]

Dear XXXX

Notification of a Data Breach

We write to advise you of a recent data breach within the Trust. Having considered the nature of the breach, we have reported this to the Information Commissioner's Office ("ICO") who will advise us of the next steps in their process. The ICO is the UK's independent body set up to uphold information rights.

The purpose of this letter is to provide you with information about the data breach, how it occurred, who it has affected, the type of information which the breach relates to, the consequences of the breach and the measures we have taken to address the breach.

Details of the breach

[INSERT DETAIL]

Name and contact details of the Data Protection Officer ("DPO")

We have an appointed data protection officer who is actively working with the Trust to address the data breach and their contact details are as follows:-

HY Education Solicitors
Sandbrook House, Sandbrook Way Rochdale
OL11 1RY
DPO@wearehy.com

The likely consequences of the data breach

[INSERT DETAIL]

Measures taken or proposed to be taken by the Trust to address the data breach

[INSERT DETAIL]

Clearly, we appreciate that you will be concerned about the data breach described within this letter. On behalf of the Trust, we sincerely apologise for any distress that this may cause. We can assure you that we are taking all necessary steps to address the situation. Should you wish to discuss this with the DPO, then please feel free to do so by telephone on 0161 543 8884 or email DPO@wearehy.com

Yours sincerely

Document History

Date	Author	Summary Changes	Approved by
October 2025	HY Education/Vicki Shelley	New Policy	Trust Board