



DATA BREACH PROCEDURE

Policy Created	February 2026
Review date	February 2027

CONTENTS

1.	Procedure statement
2.	Identifying a data breach
3.	Reporting the Breach and Immediate Steps
4.	Investigation
5.	Record of Breach
6.	Notification of a Data Breach to the ICO
7.	Notifying of data subject
8.	Centre Delegated Access Arrangements
9.	Post breach procedure
Appendix 1	Draft notification to the ICO
Appendix 2	Draft notification to the data subject

1. Procedure Statement

- 1.1 Edintervention 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 us, 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 staff, governors, directors, volunteers and contractors.
- 1.5 The Procedure will be reviewed and updated in accordance with documented review dates, though Edintervention 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:-

2.2.1 Loss or theft of personal data and / or equipment on which personal data is stored (e.g. USBs, laptops, paper files).

2.2.2 Sending personal information to the incorrect recipient whether by email, post or messaging.

2.2.3 Unauthorised access of personal information by staff, pupils or third parties.

2.2.4 Hacking or other cybersecurity compromise (e.g. phishing leading to account access).

2.2.5 Ransomware, malware infection or other forms of cyber-attack.

2.2.6 Accidental loss, alteration or destruction of personal information, whether digital or paper.

- 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 designated in an Edintervention setting who has caused, discovered or been informed of the occurrence of a data breach must notify the settings nominated data protection lead. The nominated data protection lead must notify Edintervention's nominated central contact without delay – Director of Finance and Administration (nick@edintervention.co.uk). The reported breach will be triaged by the Director of Finance and Administration, and if the breach is confirmed as a data breach, this will be immediately reported to the DPO by telephone (0161 543 8884) or email (DPO@wearehy.com). For all other staff, they should report the breach personally. If the nominated data protection lead is unavailable, setting level staff should report the breach personally.
- 3.2 The DPO will assess the data breach and advise Edintervention on any immediate action that it may need to take to address any risks arising.

4. Investigation

- 4.1 The DPO will work with Edintervention to investigate the data breach reported, taking reasonable steps to establish the following:-
- 4.1.1 When the breach occurred.
 - 4.1.2 The factual background and how the breach occurred.
 - 4.1.3 Who has been affected by the breach (e.g. staff, parents and/or pupils).
 - 4.1.4 The number of individuals affected by the breach.
 - 4.1.5 The type and sensitivity of the personal data concerned.
 - 4.1.6 The actual or potential consequences of the breach.

4.1.7 The measures taken to contain the breach.

4.2 The investigation should be completed as a matter of urgency, as its findings will determine whether the Information Commissioner's Office ("ICO") and/or affected data subjects need to be notified. Where an investigation is likely to take some time, the DPO will consider whether a notification to the ICO should be made regardless, based on the information available at that stage.

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 paragraph 6.3, and provided Edintervention notifies the DPO in a timely manner, the DPO will ensure that any notifiable data breach is reported to the Information Commissioner's Office ("ICO") within 72 hours of us becoming aware of it, using the template at Appendix 1.

6.2 If notification to the ICO is made more than 72 hours after we became aware of the breach, the report must include reasons for the delay.

6.3 If the breach is unlikely to result in a risk to the rights and freedoms of those affected, notification to the ICO under paragraph 6.1 is not required.

6.4 A data breach is likely to pose a risk to the rights and freedoms of individuals if it results — or could result — in loss of control over their personal information, limitation of their rights, discrimination, identity theft or fraud, financial loss, reputational damage, or loss of confidentiality. These examples are not exhaustive, and the DPO will assess each breach on a case-by-case basis.

6.5 Where a notification to the ICO is made, the DPO will ensure full co-operation with any requests or investigations.

7. Notifying the Data Subject(s)

7.1 Subject to paragraph 7.2, if the data breach is likely to result in a high risk to the rights and freedoms of data subject(s), we will notify them without delay using the letter template at **appendix 2**.

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

7.2.1 Edintervention has implemented appropriate technical and organisational measures, and those measures have been applied to the personal information affected, in particular measures that ensure the information is unintelligible to unauthorised persons (such as encryption) and is recoverable, e.g. where backed up.

7.2.2 Edintervention 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 important that regardless of how serious or minor the breach, lessons are learned and measures are put in place to prevent a similar incident in the future.

8.2 The measures implemented should be proportionate to the breach; however, they may include further staff training, the introduction of new or updated policies and procedures, or changes to existing security measures.

APPENDIX 1

The Information Commissioner's Office

[Insert Address 1]

[Insert Address 2]

[Insert Postcode]

[Date]

Dear [Name],

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

We write to notify the Information Commissioner's Office, in accordance with Article 33 of the GDPR, of a data breach. It is considered that this breach is notifiable as 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 within 72 hours of becoming aware of the breach. Unfortunately, we were unable to comply with this requirement for the following reasons: [INSERT DETAIL]]

Nature of the breach, affected data subjects and data records

[INSERT DETAIL]

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

HY Education Solicitors

Sandbrook House, Sandbrook Way

Rochdale

OL11 1RY

DPO@wearehy.com

Likely consequences of the breach

[INSERT DETAIL]

Measures taken or proposed to address the breach
[INSERT DETAIL]

We look forward to hearing from you in due course.

Yours faithfully

APPENDIX 2

[Name]

[Insert Address 1]

Version February 2026

[Insert Address 2]

[Insert Postcode]

[Date]

Dear [Name],

Notification of a Data Breach

We are writing to inform you of a recent data breach within the Edintervention. Having considered the nature of the breach, we have reported the incident to the Information Commissioner's Office ("ICO"), who will advise us on any further steps. The ICO is the UK's independent authority responsible for upholding information rights.

The purpose of this letter is to explain the nature of the breach, how it occurred, who has been affected, the type of information involved, the likely consequences, and the steps we have taken to address the situation.

Details of the breach

[INSERT DETAIL]

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

We have appointed a Data Protection Officer who is actively supporting us in responding to the breach. Their contact details are:

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

Likely consequences of the breach

[INSERT DETAIL]

Measures taken or proposed to be taken to address the breach

[INSERT DETAIL]

Version February 2026

We understand that this incident may cause concern. On behalf of Edintervention, we sincerely apologise for any distress this may cause. If you wish to discuss this matter, please contact the DPO by telephone on 0161 543 8884 or by email at DPO@wearehy.com

Yours sincerely