Windsor Academy Trust

Policy: Data Breach Policy and Procedure ***(To be used following an actual or suspected data breach)***	
Responsible Committee:	**Windsor Academy Trust, Board of Directors**
Date revised by the Board of Directors:	**15 July 2021**
Implementation date:	**September 2021**
Next review date:	**September 2022**

1. Introduction

1.1 Windsor Academy Trust (WAT) understands the importance of keeping personal data secure and will make all reasonable endeavours to ensure that there are no personal data breaches. This is essential for maintaining the trust and confidence of staff, pupils/students and their parents/carers when WAT uses their information. In the unlikely event of a suspected data breach, the trust will follow the procedure set out in this document. This policy and procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

1.2 All staff will receive awareness training on how to recognise a data breach as part of their data protection training and WAT's Data Protection, Information and Records Retention and Information Security and Acceptable Use Policies also contains further information.

1.3 WAT has appointed a Data Protection Officer (DPO) who is responsible for overseeing the implementation of Data Protection policies and for monitoring compliance with data protection law across the trust. The DPO details are on the WAT website. Each academy has an appointed Data Protection Lead (DPL) who should be the initial point of contact for all data protection-related matters including data breaches.

1.4 WAT is required to report certain breaches to the Information Commissioner's Office (ICO) and to data subjects under the UK General Data Protection Regulation (GDPR). There are strict timescales for reporting breaches, outlined in paragraph 3.5.

1.5 WAT also has responsibilities to report certain incidents to other regulators such as the Education and Skills Funding Agency. Section 7 covers these reporting obligations.

2. What is a data breach?

2.1 A data breach is a breach of security which leads to any of the following;

- the loss of personal data;
- the accidental or unlawful destruction of personal data;
- the disclosure of personal data to an unauthorised third party;
- the unlawful or accidental alteration of personal data; or
- unauthorised access to personal data.

2.2 Personal data is information;

- from which a person can be identified (either from the information itself or when combined with other information likely to be used to identify the person); and
- which relates to that person.

2.3 Some examples of personal data held by WAT are outlined in the WAT Data Protection Policy.

2.4 If staff are in any doubt as to whether an incident constitutes a data breach they must speak to the DPL in the academy or the DPO in the WAT central team immediately.

2.5 Please see Appendix 2 for examples of data breaches.

3. Immediate action following a data breach

3.1 On discovering that there has been a data breach/infringement you must notify the DPL immediately who will contact the DPO. The DPO will consider whether personal data has been accidentally or unlawfully;

- lost
- stolen
- destroyed
- altered
- disclosed or made available where it should not have been
- made available to unauthorised people.

3.2 The DPO will make an initial assessment of the information contained in the report as outlined in Appendix 1. A template form is available from the DPO.

3.3 The DPO will assess whether the breach may need to be reported to the ICO and the individuals affected using the ICO's self-assessment tool

3.4 It will be important to;

- identify what personal data is at risk;
- take measures to prevent the breach from worsening e.g. changing password/access codes, removing/deleting an email from inboxes which was sent by mistake;.
- recover any of the compromised personal data e.g. use back-ups to restore data;
- consider whether any outside agencies need to be informed as a matter of urgency e.g. the police in the event of a burglary or Children's Services where the breach may lead to serious harm; and
- consider whether any affected individuals shall be told about the breach straight away. For example, so that they may take action to protect themselves or because they would find out about the breach from another source. Please note this is different to the mandatory notification to individuals which does not need to be an immediate notification.

3.5 Where the ICO must be notified, the DPO will do this in accordance with the ICO guidance, via the **'report a breach'** page of the ICO website, or through its breach report line (0303 123 1113), **within 72 hours** of the awareness of the breach. As required, the DPO will set out:

- 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

3.6 If all the above details are not known, the DPO will report as much as they can **within 72 hours** of the awareness of the breach**.** 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.

3.7 Depending on the outcome of the self-assessment and the seriousness of the breach, the DPO will recommend to the Chief Operating Officer (COO) whether or not there is also a need to form a Data Breach Response Committee. Additional information that can be used to consider and assess the risk is held at Appendix 3.

3.8 The DPO will document all actions and decisions in case these are challenged at a later date by the ICO or an individual affected by the breach. The details will be entered onto WAT's Data Breach Register held centrally and will consider and follow up on any recommendations or actions outlined in the response from the ICO relating to reportable breaches, as necessary.

3.9 The DPO will liaise with the DPL who is responsible for ensuring that the Headteacher and members of the Executive team are kept informed on the actions being taken.

4. Data Breach Response Committee Roles and responsibilities

4.1 As outlined in para 3.7, the DPO will consult with the COO to determine an appropriate level of investigation and response to the data breach. The COO will identify whether there is a need to establish a Data Breach Response Committee and which individuals are needed to form the Committee. This will depend on the severity, impact, nature and location of the breach and the potential implications. Representation may be required from a number of stakeholders and the members of this committee will have certain responsibilities. Below is an outline of the areas that may need to be represented and the responsibilities that will need to be considered:

Role	**Responsibility**
The DPO/DPL in consultation with the COO	Will be notified of all breaches and will establish the Data Breach Committee if required as soon as possible once a data breach has been notified. The DPO/DPL will chair the Committee and is responsible for coordinating the response to any breach. In addition, the DPO/DPL will lead on any physical security measures which are required at the WAT site to contain the breach. The DPO/DPLare responsible for ensuring that WAT insurers are notified and for liaising with them, as required.
The Headteacher/Senior Leader	The Headteacher/Senior Leader will be responsible for any communications with staff**,** pupils/students and parents/carers and for any staff, pupil/student welfare or disciplinary considerations. The Headteacher will update the Local Advisory Body (LAB) as appropriate.

The HR Lead	The HR Lead will lead on any employee welfare or disciplinary issues in consultation with the Headteacher/Senior Leader.
The IT Lead	The IT Lead will be responsible for ensuring the security of WAT's IT infrastructure. In addition, for taking any possible technical measures to recover personal data or to contain a data breach.
CEO/Chair of Board of Directors	The CEO will liaise with the Chair of the Board of Directors as appropriate. Any decision to report the data breach to the Education and Skills Funding Agency will be taken by the CEO in consultation with the Chair of the Board of Directors.

4.2 The DPO will ensure that the WAT Executive is informed of any data breaches considered by the Data Breach Committee within the Trust.

5. Containment and recovery

5.1 As soon as a data breach has been identified or is suspected, steps must be taken to recover any personal data and to contain the breach. For example, WAT may need to;

- change any passwords and access codes which may have been compromised;
- inform employees to notify their bank if financial information has been lost (or other information which could lead to financial fraud) and offer credit protection;
- limit staff and/or pupil access to certain areas of the WAT, IT network;
- use back-up tapes to restore lost or damaged data;
- take any measures to recover physical assets e.g. notifying the police or contacting third parties who may have found the property;
- notify its insurers; and
- take action to mitigate any loss.

5.2 The DPO/Committee shall decide what action is necessary and which member(s) of the Committee will be responsible for the different aspects of the containment and recovery. Where appropriate the Committee will delegate tasks to other members of staff with the relevant expertise.

5.3 The DPO/Committee shall seek assistance from outside experts if appropriate to effectively contain the breach and recover any personal data. For example, legal advice, reputation management advice or specialist technical advice.

6. Contacting affected individuals

6.1 WAT is required to report a data breach to the individuals whose data has been compromised where the breach is likely to result in a high risk to the rights and freedoms of individuals.

6.2 The duty to tell an individual about a breach does not apply if:

- appropriate technical and organisational measures have been implemented which were applied to the personal data affected by the breach (for example the data has been securely encrypted);
- subsequent measures have been taken which will ensure that any high risk to the rights and freedoms to individuals is no longer likely to materialise; or
- it would involve disproportionate effort.

6.3 It may not always be clear which individuals shall be notified, for example, parents/carers may need to be notified rather than their children.

6.4 If WAT decides not to notify individuals this decision must be documented.

6.5 If a notification is sent this must be done so without undue delay. WAT shall work with the ICO in the case of a reportable breach in determining when is the most appropriate time to notify the individuals. Other outside agencies, such as the police, may also have a view regarding the timing of this notification.

6.6 The ICO may advise or require WAT to notify individuals. In addition, the ICO has the authority to require a more detailed notification to be given to individuals. The ICO is given these powers under the UK GDPR.

Content of the notification to individuals

6.7 The notification to individuals must include the following as a minimum:

- the name and contact details of the DPO who can provide more information;
- a description of the likely consequences of the data breach; and
- a description of the measures taken or proposed to be taken by WAT to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

6.8 In addition, WAT must consider if any additional information would be helpful to data subjects. For example, instructions on measures which they can take to protect their data now or in the future.

6.9 The notification must be drafted in clear language. If directed at pupils/students the notification shall be age appropriate.

6.10 The DPO/Committee shall advise on the most appropriate method of communication for the notification. Factors to consider include the urgency of the notification. For example, it may be appropriate to telephone individuals followed up with an email.

7. Serious Incident Report to the Education and Skills Funding Agency

7.1 An academy trust's funding agreement makes it clear that the Charity Commission's guidance on serious incident reporting must be followed by academies and, accordingly, that serious incidents shall be reported to the Education and Skills Funding Agency (ESFA), as the principal regulator of academies, as soon as possible. Where there has been a data breach, WAT will need to consider whether to make a serious incident report to the ESFA.

7.2 Directors shall consider the Charity Commission's guidance on reporting serious incidents and in particular, the examples of what to report in the "Data breaches or loss" section of their table of examples.

7.3 The ESFA has extensive information sharing powers with other regulators, like the ICO, so the ESFA may be aware if a serious incident report is not made. This does not absolve WAT of the obligation to make a serious incident report; rather it increases the likelihood of the ESFA detecting a failure to do so.

7.4 Because of the breadth of the Charity Commission's criteria for making serious incident reports, Directors shall consider whether to make a report in light of the data breach and surrounding circumstances - even where it has not been necessary to notify the ICO.

8. Notification to the police

8.1 WAT shall consider whether the police need to be notified about the data breach because it is possible that a criminal offence has been committed. However, there is no legal obligation to do so. The following are examples of breaches where a criminal offence may have been committed:

- theft (e.g. if a laptop has been stolen);
- if a staff member has shared or accessed personal data where this was not required as part of their professional duties (e.g. a staff member shares information about a pupil of famous/high profile parents with the local press);
- WAT's computer network has been hacked (e.g. by a pupil/student or a third party).

8.2 Depending on the nature of the data breach it may also be necessary to contact Action Fraud. Action Fraud is the national fraud and cybercrime reporting centre. It can be contacted on 0300 123 2040 or using www.actionfraud.police.uk

9. Internal Breach Register

9.1 The DPO is responsible for maintaining a central register of all data breaches including those which do not meet the threshold to be reported.

10. Evaluation

<u>Evaluation of WAT's security measures</u>

10.1 On an ongoing basis, WAT will seek continuous improvement in the measures that are put in place to reduce the risk of data breaches. It will take account of any lessons learned from data breaches to prevent further recurrences.

10.2 Organisational measures include:

Policies for staff on their data protection obligations, including when working away from the academy and other WAT sites;
- Guidance for staff on how to use specific computer applications and software securely; and
- Data protection training for staff.

10.3 Technical measures include:

- The use of encryption;
- Limiting access to certain areas of WAT's IT network;
- Firewalls and virus protection; and
- The use of backups.

10.4 Further information is outlined in WAT's Information Security and Acceptable Use Policy for Staff.

11. Monitoring and review

11.1 The DPO shall ensure that this policy is regularly reviewed and updated as required in conjunction with WAT Data Protection-related policies.

Appendix 1

Data Infringement/Breach (initial assessment)

1. What has happened?

Outline as much as you can about what happened and how it happened. How and when it was realised that this had occurred.

2. How and when did you discover there had been an error/potential breach?

What data was included and to whom did the data refer to (i.e. pupils and parents/other contacts). Whose data was it and who has seen it?

3. Number of personal data records concerned and how many data subjects could be affected:

4. How many subjects have actually been affected?

5. Potential consequences

Outline the possible impact and consequences on the data subjects, as a result. Has there been any actual harm caused to anyone?

6. Taking action

Outline the actions that have been taken to fix the issue and mitigate the adverse effect once the issue had been identified.

7. Follow up

Outline the steps being taken to prevent a recurrence and when this has/is expected to be completed by.

8. Details of any communication planned/actual to (or from) the data subjects affected. (NB this should be on the advice of the DPO)

9. Any other contacts involved (e.g. Third Parties?)

10. Any further information considered relevant

Name: **…….**

Date: **……..**

Appendix 1 Examples of data breaches and the next steps

Example of breach	Containment and Recovery	Establishing and Assessing the Risks	Notification	Evaluation of WAT's response to the data breach
A staff member leaves papers containing information about pupils' academic performance on a train. The papers were not in a locked case.	WAT shall find out if it is possible to retrieve the papers. For example, by calling the train company's lost property department.	The DPO will undertake an initial assessment and may convene a Data Breach Committee and may work through the questions in Appendix 2 3 as a guide below.	If the papers are not retrieved then this breach may-need to be notified to the ICO. Whether a notification to the pupils/students and their parents/carers is required will depend upon the nature of the personal data.	WAT shall work through the policy above.
Ransomware locks electronic files containing personal data.	WAT shall have a back-up of the data and shall also ensure that its systems are secured (e.g. that the ransomware has been removed).	Ditto	Depends on factors such as whether WAT was able to recover the data and whether there is any other risk to WAT's systems.	Ditto
Sending an email containing personal data to the incorrect recipient.	Use the recall email feature if available. Consider calling the unintended recipient and asking them to delete the email.	Ditto	Depends on the sensitivity of any personal data contained in the email, whether the unintended recipient has agreed to delete it etc.	Ditto

Appendix 2 Establishing and Assessing the Risks Presented by the Data Breach

	Question	**Response**
1.	What data has been (or is thought to have been) lost, damaged or compromised?	
2.	Is any of the data Critical Personal Data (Special Category Data) as defined in WAT's Data Protection Policyand Information Security and Acceptable Use Policy This would be: i. information concerning child protection matters; ii. information about serious or confidential medical conditions and information about special educational needs; iii. 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); iv. financial information (for example about parents and staff); v. information about an individual's racial or ethnic origin; and vi. political opinions;	

	vii. religious beliefs or other beliefs of a similar nature; viii. trade union membership; ix. physical or mental health or condition; x. genetic information; xi. sexual life; xii. information relating to actual or alleged criminal activity; and xiii. 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.	
3.	Who are the affected individuals e.g. staff, parents, pupils, third parties?	
4.	How many individuals have definitely been affected and how many potentially affected in a worst case scenario?	
5.	What harm might be caused to individuals (not to WAT)? The individuals do not necessarily need to be those whose personal data was involved in the breach. Harm shall be interpreted broadly, for example to include: (a) distress;	

	(b) discrimination; (c) loss of confidentiality; (d) financial damage; (e) identity theft; (f) physical harm; and (g) reputational damage.	
6.	What harm might be caused to WAT? For example, reputational damage and financial loss.	
7.	What mitigating factors may have lessened the risks presented by the breach? The following questions may assist when considering this point. (a) Were any physical protections in place to limit the impact of the breach e.g. was the data contained in a locked case when it was lost/stolen? (b) Were any technical protections in place e.g. was the data protected by encryption? (c) Have measures been taken to contain the breach e.g. have banks being notified where financial information has been compromised? (d) Have measures been taken to recover the data e.g. has lost data been found before being	

	seen by any unauthorised party or have back-ups been used where electronic information was lost or damaged?	

Appendix 3 External advice

Legal advice

WAT shall consider taking legal advice in relation to the following. Please note that this is not an exhaustive list but shall be used as a guide.

1. Determining whether to notify the ICO and the data subjects.
2. Drafting the notification to the ICO and the data subjects.
3. Drafting a serious incident report to the Education and Skills Funding Agency.
4. Any correspondence with other external agencies such as the Department for Education.
5. Any communications with the police.
6. The decision to notify WAT's insurers.
7. Any communications with staff members, pupils and parents.
8. Any disciplinary action in relation to pupils or staff.
9. Establishing whether there is a risk that an affected individual might bring a legal claim against WAT.

Reputation management

WAT shall consider obtaining advice regarding reputation management. This advice may be provided by solicitors or by other specialists. As above, this is not an exhaustive list but shall be used as a guide.

The following circumstances in particular may require specialist advice:

1. If the data breach becomes widely known to the parental community.
2. If news of the breach becomes known outside of WAT community.
3. If the media report on the breach or ask WAT for a statement.
4. If the ICO take enforcement action which may become public knowledge.

Appendix 4 Tactical and supplemental considerations

This appendix shall be completed to assist WAT in checking that all issues surrounding the data breach have been considered. It is not an exhaustive list but may assist the Committee when handling the consequences of the data breach.

Supplemental issue	Considerations
Pupil/Student welfare	
Staff welfare	
Parental/Carer complaints	
Staff disciplinary action	
Pupil/Student disciplinary action	
Reputation management	
Risks of legal claims	
Possible ICO action	

Appendix 5 Data Breach Register

Under the GDPR WAT is required to keep a record of all personal data breaches even if the breach does not meet the threshold to be reported to the ICO. The table below will be used as a basis for WAT's register. This register must be kept highly confidential and only be accessed by those staff who need to use it. Please note that the ICO may request to see this register to check that WAT is complying with its obligations under the GDPR.

Date of breach	Outline of facts	Effect of the breach	Remedial action taken	Regulatory bodies informed if any e.g. ICO