



(To be used following an actual or suspected data breach)

<i>(To be used following an actual or suspected data breach)</i>	
	People and Culture Committee
	19th September 2024
	September 2024
	September 2025

0.

- 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
produced by the In

Appendix 1

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

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?

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

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

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

(NB this should be on the advice of The DPO)



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.

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.

WAT shall work through the policy above.

Whether a notification to the pupils/students and their parents/carers is required will depend upon the nature of the personal data.

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)

	<ul style="list-style-type: none"> 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). <p>If any of these types of data are involved this makes the breach more serious.</p>	
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.	<p>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.</p> <p>Harm shall be interpreted broadly, for example to include:</p> <ul style="list-style-type: none"> (a) distress; 	

- (b) discrimination;
- (c) loss of confidentiality;
- (d) finan

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

This appendix shall be completed to assist WAT in checking that all issues surrounding the data breach have

g

assign

the data breach

u
