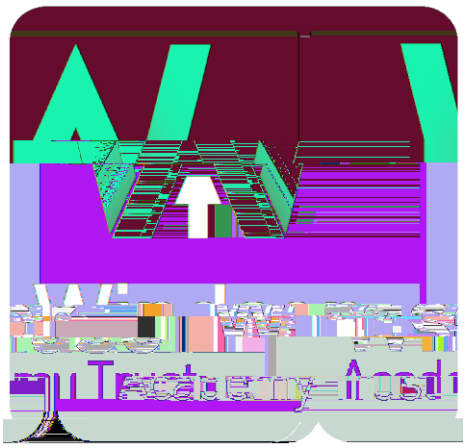

(To be used following an actual or suspected data breach)	
	People and Culture Committee
	13th July 2023
	September 2023
	September 2024

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 immediately.

2.5 Please see Appendix 2 for examples of data breaches.

.

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.

coerse. note

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. The DPO (Judicium Education) will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals. This will be done without undue delay and where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (i.e., it is not 72 working hours). If the School is unsure of whether to report a breach, the assumption should be to report it. Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

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

	responsible for ensuring that WAT insurers are notified and for liaising with them, as required.
The Headteacher/Senior Leader / Director of	

7. An academy tr s funding agreement makes it clear t Charity C guidance on s us incident reporting must be followe ademies accordingly, th erious incidents shall be reported to cation ar Funding Agenc ESFA), as the principal regulator of a es, as so possible. Whe here has been a data breach, WAT w to consi make a serious incident report to the ESFA.

7.2 Directors shall consider the Charity Commission's guid incidents and in particular, the examples of what to rep s section of their table of examples.

7.3 has extensive information sharing powers w r regulators, like the ICO, so th ESFA may be aware if a serious incident re not made. This does n ab olv WAT of the obligation to make a serious in eport; rather it increases the likelihood of the ESFA detecting a failure o.

7.4 Because of the breadth of the Charity Commission's cr r making serious incident reports, Directors shall consider whether to ma rt in light of the data breach and surrounding circumstances - even where it t been necessary to notify the ICO.

8.1 WAT s

.

K

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

	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: distress;

discrimination;

loss of confidentiality;

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 been considered. It is not an exhaustive list but may assist the Committee when handling the consequences of the data breach.

Pupil/Student welfare

Staff welfare

Parental/Carer complaints

Staff disciplinary action

Pupil/Student disciplinary action

Reputation management

Risks of legal claims

Possible ICO action