Information Security Incident Reporting Policy

This policy has been subject to an Equality Impact Assessment by:

Author/Reviewer: Lyle Nicholson

SLT/EET:

Governors/Trustees:

Could/does the policy or procedure have a negative impact on one or more of the groups of people covered by the protected characteristics of equality? If so, how can this be changed or modified to minimise or justify the impact? no

Could/does the policy have the potential to create a positive impact on equality by reducing and removing inequalities and barriers that already exist? If so, how can these be maximised? no

Introduction

This policy has been written to govern Tees Valley Collaborative Trust (and its academies) management of information security incidents and data breaches.

Queries about any aspect of the Trust's Information Governance strategy or corresponding policies should be directed to the Data Protection Officer at SchoolsDPO@veritau.co.uk

Scope

This policy applies to all the Trust's employees, any authorised agents working on behalf of the Trust, including temporary or agency staff, elected members, and third party contractors. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

They apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

Article 33 of the GDPR requires data controllers to report breaches of personal data to the Information Commissioner's Officer, and sometimes the affected data subject(s), within 72 hours of discovery if the incident is likely to result in a risk to the rights and freedoms of the data subject(s). Therefore it is vital that the Trust has a robust system in place to manage, contain, and report such incidents. The

Information Security Incident Management Policy details how the Trust will handle and manage information security incidents when they arise.

Notification and Containment

In order for the Trust to report serious incidents to the ICO within 72 hours it is vital that it has a robust system in place to manage, contain, and report such incidents.

Immediate Actions (Within 24 Hours)

If an employee, governor, or contractor is made aware of an actual data breach, or an information security event (a 'near-miss'), they must report it to their line manager and the Director of Resources within 24 hours. If the Director of Resources is not at work at the time of the notification then their Out of Office email will nominate another individual to start the investigation process.

If appropriate, the individual who discovered the breach, or their line manager, will make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information.

Assigning Investigation (Within 48 Hours)

Once received, the Director of Resources will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings can be found in Appendix One of this document.

The Director of Resources will notify the relevant Information Asset Owner (IAO) that the breach has taken place. The Director of Resources will recommend immediate actions that need to take place to contain the incident.

The IAO will assign an officer to investigate white, green and amber incidents. Red incidents will be investigated by the Data Protection Officer with the assistance of Internal Audit and Counter Fraud Teams.

Reporting to the ICO/Data Subjects (Within 72 Hours)

the relevant manager, Director of Resources, IAO and DPO will make a decision as to whether the incident needs to be reporting to the ICO, and also whether any data subjects need to be informed. The relevant manager/IAO will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

Investigating and Concluding Incidents

The Director of Resources will ensure that all investigations have identified all potential information risks and that remedial actions have been implemented.

When the DPO has investigated a data breach then the Director of Resources must sign off the investigation report and ensure recommendations are implemented across the academy.

The Director of Resources will ensure all investigations have been carried out thoroughly and all highlighted information security risks addressed.

APPENDIX ONE: SEVERITY RATINGS FOR INFORMATION SECURITY INCIDENTS

Rating	Incident Threshold	Recommended Actions
WHITE **Information Security Event**	No breach of confidentiality, integrity, or availability has taken place but there is a failure of the implemented safeguards that could lead to a breach in the future. *Examples* ▪ A post-it note containing a user name and password to a database is found attached to a keyboard. ▪ A key safe, containing keys to filing cabinets, has been found unlocked and unsupervised.	▪ Responsible officer(s) spoken to by management and reminded of data protection responsibilities. If repeated offence management to consider HR action. ▪ Logged on register of incidents
GREEN **Minimal Impact Incident**	The academies security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. Incident has been contained within the organisation (or trusted partner organisation). The information does not contain any special category data or any data that would be considered to be sensitive. The actual or potential detriment to individuals is virtually non-existent. *Examples* ▪ An email, containing details of a service user's address or contact details, is sent to an incorrect recipient within the academy. ▪ A document containing the only record of students contact details have been destroyed in error.	▪ Responsible officer(s) spoken to by management and reminded of data protection responsibilities. If repeated offence management to consider HR action. ▪ Logged on register of incidents ▪ Notify SIRO ▪ Investigation report to be conducted by Information Asset Owner.
AMBER **Moderate Impact Incident**	The academies security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. The information has left academies control. The information does not contain special category data or data that is considered to be sensitive but may contain data that should have been	▪ Responsible officer(s) asked to re-sit Data Protection e-learning. Management to consider HR action. ▪ Consider utilising key messages/intranet to remind all staff of certain data protection best practice.

	confidential to the academy. The incident appears to affect only a small number of individuals. The actual or potential detriment is limited in impact and does not reach the threshold for reporting to the Information Commissioner's Office. *Examples* ▪ A letter is sent to the wrong postal address and the incorrect recipient has learnt of another individual's dealings with the academy. However, the letter does not contain any special category information. ▪ An email has been sent to ten parents without the BCC function being utilised which reveals all ten personal email addresses.	▪ Logged on academies register of incidents ▪ Investigation report to be conducted by Information Asset Owner .
RED **Serious Impact Incident**	The academies security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. The information has left academies control. The information contains special category data or data that is considered to be sensitive in nature and/or affects a large number of individuals. The incident has or is likely to infringe on the rights and freedoms of an individual and has a likely potential to cause detriment (emotional, financial, or physical damage) to individuals. *Examples* ▪ A file, containing safeguarding and health data, is left unsupervised in a vehicle which is subsequently stolen and the data has been lost to persons unknown. ▪ A spreadsheet containing the SEN information for all the academies pupils has been mistakenly sent to a member of the public.	▪ Management to consider (potentially immediate) HR action. ▪ Logged on academy register of incidents ▪ Notify Data Protection Officer ▪ Consider forming an incident strategy conference ▪ Consider reporting to the Information Commissioner's Office ▪ Consider informing affected individual(s) ▪ Consider informing the police or other law enforcement agencies. ▪ Where appropriate the Data Protection Officer to conduct incident investigation with assistance (where and if required) from internal audit and counter fraud colleagues.

Date of Last Approval/Revision	
Review interval (years)	3 yearly
Responsible Officer	Director of Resources
Approval/review body	Executive Team
Date of next review	September 2024
Public File location	Tees Valley Collaborative Trust Sharepoint/ Websites/Staff Handbook