PONTEFRACT
ACADEMIES TRUST

Information Security Incident Reporting Policy

Trust Board Approval Date: 1 October 2018

Information Security Incident Reporting Policy

1.1 PURPOSE

Pontefract Academies Trust ("The Trust") is required to collect, hold, process and share information to enable it to operate. This policy is to ensure that the Trust complies with the requirements of the European Union's General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

This policy sets out the Trust procedures to be followed if anyone appointed/employed by the Trust discovers an information security incident.

1.2 SCOPE

This Policy applies to all Trust employees, agency staff, trustees, School Performance Review Board ('SPRB') members, or any other third-party contractors appointed/employed by the Trust. Individuals who are found to knowingly or recklessly infringe this policy may be subject to disciplinary or other appropriate action.

This Policy applies to information in all forms including, but not limited:

- Hard copy 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 internet and intranet; and
- Photographs and other digital images

1.3 RELATED POLICIES OR PROCEDURES

The Information Security Incident Reporting Policy should be read in conjunction with other policies and procedures that relate to conduct systems and procedures. This includes:

- Staff Code of Conduct, including safer working practice guidance
- Information Security Policy
- Information Security Incidents Reporting Policy
- Records Management Policy and Procedures
- Surveillance Policy (including CCTV)

Information Security Incident Reporting Policy

1.4 DEFINITION OF A BREACH

An information security incident is an event which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately and has caused or has the potential to cause damage to the Trust's information assets and/or reputation.

An information security incident may be confirmed or suspected.

An information security incident includes, but is not restricted to:

- Loss or theft of confidential or special category data, or portable equipment/paper which such data is stored/recorded
- Equipment theft or failure
- Unauthorised use, access or modification of data or information systems;
- Attempts (failed or successful) to gain unauthorised access to information or IT systems
- Unauthorised disclosure of special category and confidential data;
- Website defacement
- Hacking attack
- Loss as a result of fire or flood
- Human error
- Deception – obtaining or attempting to obtain information through imitation

1.5 NOTIFICATION AND CONTAINMENT

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

1.6 IMMEDIATE ACTION (WITHIN 24 HOURS)

If an employee, trustee, SPRB member, 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, the Head of School, and the Director of Operations within 24 hours.

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

1.7 **ASSIGNING INVESTIGATION (WITHIN 48 HOURS)**

Once received the Head of School in liaison with the Director of Operations will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings are:

Severity	Analysis	Action Required
WHITE	**Information Security Event** No breach has taken place but there is a failure of the implemented safeguards that could cause a data breach in the future	**Log & send a reminder to employees** **Examples:** • Emails sent to the wrong person but does not contain personal data • Found post-it note with user name & password but has not been used for any known detriment
GREEN	**Minimal Impact** A data breach has occurred but has been contained within the organisation (or trusted partner organisation), the information is not considered to be particularly sensitive, and no further action is deemed necessary	**Conduct an Internal Investigation** **Examples:** • Emails that contained personal data, sent to the wrong member of staff but kept within the organisation and no harm caused • Information on child's file is incorrect/mixed up.
AMBER	**Moderate Impact** Security measures have failed and consequently have resulted in the loss, release, or corruption of personal data. However, the actual or potential detriment is limited in impact and does not reach the threshold for reporting to the information commissioner's office.	**Action: Conduct an internal investigation** • Letter sent to the wrong parent revealing a fact about another child but not considered sensitive enough to warrant detriment. • Lost information about a child's progress**.**

Information Security Incident Reporting Policy

RED	**Serious Impact** A breach of security involving sensitive personal data and/or a large volume of personal data. The incident has or is likely to cause serious detriment (emotional, financial, or physical damage) to individuals concerned. The breach warrants potential reporting to the information commissioner's office and urgent remedial action. HR input may also be required.	**Action: Contact the DPO ASAP** • Safeguarding information has been disclosed to the wrong parent • Lost medical information about a child (such as life threatening allergies).

1.8 The Head of School will notify the relevant Information Asset Owner that the breach has taken place. The Head of School will recommend immediate actions that need to take place to contain the incident.

The Information Asset Owner will investigate white, green and amber incidents. Red incidents will be investigated by the Data Protection Officer with the assistance of the Trust internal audit service and counter fraud teams as appropriate.

1.9 **REPORTING THE BREACH TO THE ICO/DATA SUBJECTS (WITHIN 72 HOURS)**

The Head of School in liaison with the Director of Operations, and Data Protection Officer will make a decision as to whether the incident needs reporting to the ICO, and also whether any data subjects need to be informed. The Head of School will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

1.10 **INVESTIGATING AND CONCLUDING INCIDENTS**

The Head of School 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 relating to a specific school then the Head of School must sign off the investigation report and ensure recommendations are implemented in their school. If a data breach relates to an incident across the Trust or in the Trust HQ then the Chief Executive Officer must sign off the investigation report and ensure recommendations are implemented across the Trust.

The Head of School in liaison with the Director of Operations will ensure that all investigations have been carried out thoroughly and all highlighted information security risks addressed.

1.11 RETAINING A REGISTER OF BREACHES

The Director of Operations will maintain a register of all information security breaches across the Trust.

Appendix A: Information Security Incident Investigation Form

PART ONE: INCIDENT MANAGEMENT							
1.	Incident Reference Number						
2.	Date of Incident						
3.	Date of Discovery						
4	Severity Rating	Green		Amber		Red	
5	Has this been reported to the DPO	Yes			No		
	5.1 If Yes Date Reported						
	5.2 If No reason not reported						
6.	Has this been reported to the ICO	Yes			No		
	6.1 If Yes Date Reported						
	6.2 If No reason not reported						
7.	Has this been reported to the Data Subject?	Yes			No		
	7.1 If Yes date reported						
	7.2 If No reason not reported						

PART TWO: CONTAINMENT AND RECOVERY		
1.	Does the information include personal data and if so what personal data was included? i.e. are one or more individuals identified or identifiable?	
2.	Does the information include special category personal data and if so what special category data was included? Ethnic or racial origin; religious or philosophical beliefs; political beliefs, trade union membership, physical or mental health, sex life or sexual orientation criminal offence or conviction history, genetic data, biometric data	
3.	How many individuals does this or will this effect (estimate)	
4.	Have you regained control of the information (Yes / No / In Part)	
	4.1 If Yes/Partial when and how?	
	4.2 If not are you satisfied that further disclosure will not occur – e.g. if the document has been deleted?	
	4.3 If yes, when and how did you get confirmation of this?	
	4.4 If no, what other steps have been taken to prevent further disclosure?	

Appendix A: Information Security Incident Investigation Form

PART THREE: FURTHER ACTION AND INVESTIGATION		
1.	What caused the incident? Please provide as much information as possible. Human error is not an explanation – if there was no external or other cause, were there unusual workload issues, or interruptions, or lack of training or support?)	
2.	What measures have been taken to prevent, or reduce the risk of, recurrence?	
3.	Has any disciplinary action been considered or taken? If so, what, and with what outcome?	

PART FOUR: EVALUATION AND RESPONSE		
1.	What lessons can be learned corporately from this incident?	
2.	Has an improvement plan been devised? If so please attach a copy	
Other comments or necessary information		

Investigating Officer (Name)	
Investigating Officer (Job Title)	
Date Investigation Completed:	

Data Protection Officer Analysis (if passed to the DPO)	
DPO Name	
Date Opinion Given	

The DPO will retain a copy of this incident report for six years after closure of the case. The Trust will also keep a copy of this report for its own records.