Information Security Breach Procedure

September 2018

The Learning Community Trust Information Security Breach Procedure (ISBP) v3.4

What to do in the event of a possible data breach/incident

1. Introduction

1.1 This procedure supports the Trusts Information Security Policy and **must be read in conjunction** with it. This procedure details the necessary steps to take if you have concerns that there has been a breach of personal identifiable information (PII – see 1.2 for examples) by staff, Governors, Trustees or third parties[1].

1.2 Some typical examples of PII include, but are not limited to:-

- **Personal Data –** e.g. name; address; telephone number; date of birth; NI number; bank account details
- **Sensitive/Special Personal Data –** e.g. information specifically relating to physical or mental health or condition; race or ethnicity; political opinions; religious beliefs, or beliefs of a similar nature; membership of a trade union or non-membership;; sexual life; commission or alleged commission of an offence;

1.3 The principles of securing information (in accordance with Principle 7 of the Data Protection Act and principle 6 of the General Data Protection Regulations from May 2018), can be found in the Information Security Policy.

2. What is a possible breach of PII?

2.1 A breach of PII is where identifiable personal information has been or has the potential to be:

- Viewed or copied by an individual unauthorised to do so,
- Communicated to an unauthorised individual/organisation, e.g. sent to wrong address and opened/read
- Lost or stolen

There are many examples of what constitutes a possible data breach, typical examples are detailed below:

- Loss of mobile phone/laptop or other ICT equipment
- PII being emailed/posted/faxed to an unintended recipient or address and read by the individual, e.g. a letter containing safeguarding information or financial information about an individual being sent to 36 Smith Street instead of 63 Smith Street (the intended recipient) and opened
- Loss of information/records relating to individuals and read by an unauthorised person, e.g. a lost file containing personal grant information
- Viewing PII on an ICT system that you do not need to access as part of your role
- Not keeping information secure; i.e. leaving correspondence on your desk at the end of the working day

2.2 There may be security incidents where PII has been given to an unauthorised person (due to a human or procedural error) but the recipient has not opened/read the PII. The PII has then been returned or it has been confirmed that it has been destroyed. Cases such as these should be notified to Chief Operating

[1] Third parties could include temporary employees, agency workers, volunteers, partners or contracted service providers

Officer/Data Protection Officer who will undertake an investigation into the security incident and implement actions that will minimise the possibility of a similar incident in the future.

3. What should I do if I become aware of a possible data breach?

3.1 Outside a normal working day

3.1.1 If you become aware of a possible data breach you should report it immediately where you can. If this occurs outside normal working hours, e.g. bank holidays, weekends, etc., please contact your Line Manager within 12 hours of the incident occurring.

3.2 Normal working day

3.2.1 If a breach occurs or you suspect one has occurred you will need to inform your line manager (who will inform the relevant Principal/Head Teacher) immediately (or as a minimum within 12 hours of incident occurring). The matter must then be forwarded to the Trust within 24 hours of the incident occurring for recording and investigation.

3.2.2 If the incident involves theft or a crime then you should contact the police and report this. Please make sure you obtain and record a crime reference number from the police where applicable.

3.2.3 If the incident involves the loss or theft of ICT equipment then this should also be logged with the ICT Service Desk.

3.2.4 When the matter is reported to the Trust and ICT (where relevant) the following information as a minimum should be to hand:

- Crime reference number given to you by the police (if applicable)
- Police station and constabulary the incident was reported to (if applicable)
- Place, time and date(s) the incident occurred
- Staff member and/or team(s) or 3rd party suppliers involved
- A summary of the information that has been lost, stolen or incorrectly communicated
- A list of the individuals affected or that could be at risk
- A list of organisations that may need to be contacted (e.g. shared service information), if applicable
- Confirmation as to who else in the authority has been informed, e.g. Headteacher, Principle

3.2.5 When the incident is reported to Trust they will:

- Assess the level of the risk associated with the incident
- Contact the Data Protection Officer (DPO) Service/Support
- Agree the immediate mitigating actions that should take place and who should undertake them including who else needs to be informed (internally and externally)
- Agree who will undertake an investigation into the incident – low risk will be the service area; medium – area/DPO by agreement; high risk – DPO.
- Compare the incident against notification rationale outlined by the Information Commissioners Office (ICO) and notify (after approval by the SIRO) if applicable
- Produce or agree the production of an incident report, see ***Appendix 1*** for required layout
- Agree remedial action to be taken by the relevant area
- Communicate any lessons learnt across the Trust where appropriate

3.2.6 Managers can obtain guidance on possible action to be taken in relation to employees implicated in data breaches by accessing the relevant Human Resources guidance document.

Appendix 1

Suggested Report Template

(Input in grey below are example entries only)

Tick relevant box

Breach?	?	**Incident?**	

See section 2 of ISBP for guidance on what constitutes a breach or incident

Date Occurred	*10/12/18*	**Officer Implicated**	*R Montgomery*

Date when Principle/Head informed	**Was breach/incident identified as a result of a customer complaint (Y or N?)**	*Y*
Informed Jenny Marriott on 10/12/12/18 - Suzanne Dodd		

Categories of Data Breached	**Number of Individuals Affected**	**Number of Records Breached**
Name, Address, Bank details	*1*	*6*

Description of breach/incident (including the type of information and date/location of incident)

Bank statements collected for identification purposes returned to 15 Darby Road on 10/12/18 instead of correct address 51 Darby Road

Reported to police Y/N?	*N*	Date Reported / Police Station	*N/A*	Crime number	*N/A*

Has information been returned to Trust or destroyed?	Do you intend to notify the data subject(s) affected? If YES please consult DPO prior to doing this If NO please give an explanation for this
Information returned to Trust on 12/12/18	*Yes – as they will be able to ask their bank to watch their account*

How did breach/incident occur?
Officer had incorrectly updated the contact record for this customer

Measures already taken to address breach
1. Procedures for updating contact records reissued to all staff
2. Warning of this incident emailed to all staff
3. QA checks to be put in place monitoring contact records accuracy

BELOW SECTIONS TO BE COMPLETED ONCE INVESTIGATION ENDED

Description of action (if any) taken against officer implicated in the breach/incident
Informal discussion with SDM and warning about future conduct

Lessons learnt to be implemented (if relevant)

1. Procedures for updating contact records reissued to all staff
2. Warning of this incident emailed to all staff
3. QA checks to be put in place monitoring contact records accuracy

Document Version Control

Version	Date	Author	Sent To	Comments
3.0	25/7/17	R Montgomery	Corporate Information Security Group, SIRO (JE) and HR SDM (SW)	Sent draft/updated version including GDPR requirements for initial comment
3.1	16/8/17	R Montgomery	J Eatough / S Dodd	This version includes changes suggested by K King
3.2	17/8/17	R Montgomery	S Wright, IG Team	This version includes changes suggested by J Eatough
3.3	05/09/17	R Montgomery	Corporate - published	Final version
3.4	01/08/18	P Jones	LCT	Adopt for LCT use