Procedures for Reporting and Handling Security Incidents

Title	Procedures for Reporting and Handling Security Incidents
Author/Owner	Simon Pringle
Status	Draft
Version	Major
Date Approved	21st May 2018
Approved by	
Review Date	May 2019
Security Classification	OFFICIAL

Contents

1. Introduction

1.1. This document applies to everyone who undertakes duties on our behalf (including third parties, suppliers, partners and contractors etc.). We have a duty to ensure that the information we process and hold is secure. We will react appropriately to any actual or suspected security incidents relating to information, systems and data.

1.2. We recognise there are risks associated with individuals accessing and handling information in order to conduct our business and have in place Policy and Procedures which need to be followed. Security incidents occur when those policies are not followed. Therefore there is a need to report these incidents to manage the risks and identify improvements to decrease the number of future incidents.

1.3. Where an external supplier has reported a security incident it is the responsibility of the business area for which they are providing a service to report the incident.

2. Policy References

2.1. This procedure is a requirement of the following policies:

- Security Incident Policy

3. Procedures

3.1. What is a Security Incident?

3.1.1. An **information security incident** is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of information and weaken or impair business operations.

3.1.2. An **information security event** indicates that the security of an information system, service, or network may have been breached or compromised. An information security event indicates that an information security policy may have been violated or a safeguard may have failed.

3.1.3. See Appendix C: Incident Types for a comprehensive list of what is considered a breach. There are some examples below:

- Using, or being asked to use, another person's login or password (or both)
- Not locking your PC/ laptop before leaving it,
- if you are logged in;
- Allowing confidential information to be passed on to people who do not have the correct authorisation to see it or not preventing this;

- Sending personal information to the wrong recipient, either by email, post or fax;
- Stolen or lost electronic equipment, including laptops or mobile phones;
- Sending abusive emails, or forwarding racist or sexist jokes or emails;
- Allowing someone to enter the building without an appropriate pass;
- Intentional or accidental infection of computer viruses or unauthorised software.
- Loss or theft of financial information, e.g. credit card data.

3.2. Employee Responsibilities

3.2.1. Anyone discovering a security incident, even those they think are minor, must immediately report it to the DPO.

3.2.2. No retaliatory action will be taken against any member of staff who reports a security incident about another member of staff in good faith, regardless of the seriousness of the security incident or the level of individual responsible for the breach. Identification of a reporting party who requests anonymity shall be protected to the degree feasible, but cannot be guaranteed.

3.3. Investigations

3.3.1. The ICT technician will classify the security incident using the scoring system at Appendix A, and will then refer it to the DPO. The DPO will contact the SIRO for major incidents to ensure they can assess and recommend report the SIRO reports the matter to the ICO if required. Full details of the roles and responsibilities for investigating a security incident can be found in Appendix B**.**

3.4. Timescales

3.4.1. The DPO will contact the relevant service area within 4 working hours of being notified of the incident, and will agree initial actions to be taken. Depending on the complexity of the incidents the timescales for completing investigations will vary. Security Incident Classifications can be found in Appendix A. However, listed below are the expected timescales for the majority of incidents to be investigated and closed:

- **Minor/Near Miss (Scale** = **1)** – closure within 1 week
- **Medium (Scale = 2)** – corrective action within 24 hours, investigation of cause of incident, implementing preventative action and outcome report within 2 weeks
- **Major (Scale = 3)** – corrective action within 24 hours; investigation of cause to begin immediately and implementing preventative action,

including recommendations to Leadership Team and outcome report to be completed within 1 month.

3.5. Reporting to the ICO

3.5.1. The Information Commissioner requires major breaches of Data Protection law to be reported, and from the 25th May 2018, the General Data Protection Regulations (GDPR) these requirements are increased.

3.5.2. It is the Senior Information Risk Owner's (SIRO) responsibility to decide whether to report a breach to the regulator; the Information Commissioner's Office (ICO).

3.5.3. The ICO state that they require notification of breaches where the incident "is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage". Each case must be assessed on a case by case basis and should involve the opinion of the Data Protection Officer

3.5.4. If the breach is consider to represent a 'high risk' to the data subject rights (i.e. it is a higher level of risk still than that requiring reporting to the ICO), then there is a further requirement that the data subjects themselves are formally notified by the Organisation. The opinion of the Data Protection Officer should be taken into account by the SIRO.

3.5.5. If the ICO is to be notified about the breach, the notification must contain:

- The nature of the breach including the categories and approximate number of the:
    - individuals concerned
    - personal data records concerned
- The name and contact details of the Data Protection Officer or other contact point where more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach
- The measures taken to mitigate any possible adverse effects.

3.5.6. A notifiable breach has to be reported to the ICO under the GDPR within 72 hours of the Organisation becoming aware of it. The law recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases, however the initial notification must happen within the timescale.

3.5.7. If the breach is sufficiently serious to warrant notification to the public, the Organisation must do so without delay.

3.5.8. The reasons behind the SIRO's decision whether or not to notify must be documented on the Security Incident Outcome Report Form and must include consideration of the DPO's opinion.

4. Advice and Support

If you have any issues over the clarity of these procedures, how they should be applied in practice, require advice about exemptions from the requirements or have any suggestions for amendments, please contact head teacher at head@rbps.org.uk.

4.1.

5. Breach Statement

5.1. A breach of this procedure is a breach of Information Policy. Breaches will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Appendix A: Risk Classification

Any incident scoring 3 would be reportable to Internal Audit for consideration of further reporting to the ICO, if it scores less, it is not.

1. ***As defined by Data Protection Law, is the data:***
   - Sensitive **[1]**
   - Personal **[0]**

2. ***Has the law been breached?***
   - Yes **[1]**
   - No **[0]**

3. ***Did the data get sent:***
   - Within the organisation **[0]**
   - To an external partner organisation (NHS/ Social Care) **[1]**
   - To an external organisation/ individual **[2]**

4. Has the authority applied the appropriate technical security (e.g. is the information encrypted, appropriate access controls in place, correct procedure followed):
   - Yes **[0]**
   - No **[1]**

Appendix B: Roles & Responsibilities

ICT Technician

- Classify the Security Incident using the criteria at Annex A
- Verify the details and oversee the progress of incidents
- Work with the DPO and SIRO to investigate major security incidents and collect evidence.
- Provide advice, support and intervention as appropriate to each case.
- Review Incident Outcome Reports and close accordingly
- Following receipt of Outcome Reports analyse results looking at lessons learnt and implement required actions
- All outcome forms with actions that have future completion dates can be closed with a scheduled task created to review.

Data Protection Officer

This person is appointed to:-

- Ensure remedial action is taken within 24 hours to recover unlawful disclosure of personal/sensitive information.
- Identify expected outcomes, stakeholders and any policies or standards that may have been breached.
- Speak to staff involved.
- Preserve evidence and maintain an audit trail of events and evidence supporting decisions taken during the incident
- Engage appropriate specialist help if required
- Escalate as appropriate
- Inform data subjects (service users, employees) if necessary
- Identify and manage consequent risks of the incident (these may be service related or involve risks to service user/ employee safety, continuity of care etc.)
- Invoke disciplinary procedure as appropriate or document the reasons where it is decided not to take action where such action may be viewed as relevant by external parties
- Develop and implement an appropriate communications plan
- Institute appropriate measures to prevent recurrence
- Complete the Incident Outcome Report (Annex D)

SIRO

- Undertake the investigation of major security incidents and those escalated to them.
- Initial quick review of the security incident to establish where further information may be required.
- Work with the DPO to investigate major security incidents.
- Provides an initial notification to relevant senior management that a major incident or serious information breach has occurred.
  a. If there is a serious breach of data, they will also undertake any assessment regarding notifying the ICO about the loss.
  b. The results of this risk assessment will be circulated to the same relevant senior managers who have been notified about the incident. The decision on

   proceeding or not with contacting the ICO sits with the Senior Information Risk Owner (SIRO).
   c. Advice on the appropriate method of collecting and securing evidence.
- complete an outcome report and recommend remedial actions.

Senior Information Risk Owner (SIRO)

- Makes the final decision on behalf of the Organisation on whether the incident is of a sufficient severity to require reporting the matter to the Information Commissioner's Office

Appendix C: Incident Types

The following is a list of security incident types which fall within the scope of the Policy and this Procedure:

Categories:	Description:	Incident Types:	Description:
3rd Parties	*Breaches of Information Security Policy that affect or are caused by 3rd parties.*	Secure email	*Issue with GCSx Connection*
		VPN Misuse	*Misuse of Support VPN*
		Loss of Personal Information	*3rd party loss of personal info*
		Loss of Business Information	*3rd party loss of business info*
		Password Sharing	*3rd parties sharing passwords*
Breach of Policy	*Breaches of Information Security Policy that are not reflected in one of the other options.*	Email Misuse	*Spam emails, abusive messages, improper use of mailing lists.*
		Internet Misuse	*Accessing sites in business time, inappropriate sites, use of un-authorised online systems*
		Misuse of authority	*Misuse of position, access or identity for personal gain.*
		Personal Device	*Adding an unauthorised personal device to the network or storing ECC information on a personal device.*
		Information Handling	*General lack of good information handling*
		Insecure Password	*Password for system does not match agreed standard.*
		Staff Tailgating	*Member of staff has tailgated in a building processing data*
		GCSx	*Member of staff has abused the use of their GCSx account*
Data Protection	*Breaches of Data Protection law including loss, theft or disclosure of personal information.*	Disclosure Personal Information	*Confirmed disclosure of personal information to non-intended recipient.*
		Loss of Personal Information	*Loss of personal information with no certainty it has been disclosed.*
		Theft of Personal Information	*Theft of personal information with no certainty it has been disclosed.*

Information Complaint	*Complaints received from either the ICO or the public in relation to Information Handling Legislation.*	ICO DP Complaint	*Complaint from the ICO relating to non-compliance with the DP Act 1998.*
		ICO FOI Complaint	*Complaint from the ICO relating to non-compliance with the FOI Act 2000.*
		Public FOI Complaint	*Complaint from public relating to non-compliance with the FOI Act 2000.*
		Public DP Complaint	*Complaint from the Public relating to non-compliance with Data Protection law (DPA 1998 & GDPR 2016)*
Lost/ Stolen Equipment	*Loss or theft of equipment (no data stored).*	Lost Equipment	*Lost equipment (no personal data stored).*
		Theft of Equipment	*Theft of equipment (no personal data stored).*
Network Security	*Incidents that affect the Security of the IT Network storing data.*	Spam Email	*Spam emails received that pose a threat to the Network.*
		Mailbox Size	*Large mailbox size or large mailbox size increase within 24 hours.*
		Systems Failure	*Critical System offline.*
		Virus Threat	*Threat of virus to the network*
		Folder Permissions	*Reset or corruption of folder permissions for folders on the network*
		Encryption – Laptop	*Laptop discovered with no Encryption Software installed.*
		Encryption – Desktop	*Desktop discovered with no Encryption Software installed.*
Password Sharing	*Incidents where a password has been shared or used by another user.*	Password Demanded	*Employee has demanded password of a system from another member of staff.*
		Password Shared	*Member of staff has shared password of a system with another member of staff.*
		Logged someone in	*Member of staff has logged someone into a system under their own username without sharing the password.*
Physical Security	*Incidents where the physical security of*	Insecure Building	*Building or storage facility discovered to be insecure.*

	a building or storage space processing data is compromised.	Public Unauthorised Access	*Unauthorised person has been able to access a building or secured area.*
Lost/ Stolen Business Information	*Incidents where sensitive information has been lost, stolen or disclosed.*	Disclosure Business Information	*Disclosure of Sensitive Business information*
		Loss Business Information	*Loss of Sensitive Business information with no confirmed disclosure.*
		Theft Business Information	*Theft of Sensitive Business information with no confirmed disclosure.*

Appendix D: Outcome Report

Security Incident
Outcome Report Forr