Information Security Incident Reporting Guidance for Trusts

Introduction

The UK General Data Protection Regulation (UK GDPR) has introduced a duty on all organisations to report certain types of personal data breaches to the relevant supervisory authority (Information Commissioners Officer (ICO)).

An organisation must notify certain breaches of personal data within 72 hours. This is where the breach is likely to result in a high risk to the rights and freedoms of individuals; organisations must also inform those individuals without undue delay.

This guidance describes the process for reporting, recording and dealing with Information Security incidents.

What is a security incident?

The UK GDPR (Article 33) requires a breach to be reported where it is likely to **result in a high risk to the rights and freedoms of individuals**. Article 34 also makes it a legal obligation to communicate the breach to those affected without undue delay when it is likely to result in a high risk to individual's rights and freedoms.

There is no expectation that a full investigation will be carried out within 72 hours.

An Information Security Incident is any real or suspected event that has resulted or could result in:

- The disclosure of confidential information to any unauthorised person;
- The integrity of a system or data being put at risk;
- The availability of a system or information being put at risk;

An Information Security Incident could relate to any breach of security or confidentiality.

Examples of Security Incidents are:

- Losing a computer/device with personal information on it e.g. IPad, Laptop, Memory stick
- Giving information to someone who should not have access to it – verbally, in writing or electronically
- Using someone else's user ID and password to access a computer system
- Loss of paper documents containing personal information

Consequences

The Trust as an organisation is the data controller, not individual Trustees, teaching staff or the Data Protection Officer. The law applies to the organisation itself and it is responsible for any breach. If a breach occurs, whilst there is no guarantee enforcement action will not be used, it is a myth that a breach will automatically lead to a large fine.

A breach of Data Protection legislation could result in the Trust being fined if it is very serious. The reputation of the Trust could also be damaged, particularly, if inadequate controls have contributed to the breach. Depending on the nature of the information that has been compromised there may also be a potential Safeguarding issue.

If a breach does occur and is investigated by the Information Commissioner (ICO), the first step they will take is to ascertain what was in place at the Trust to prevent the breach from happening in the first place (e.g. Trust policies, procedures). If there is a clear record of what measures have been taken, a proportionate approach will be taken by the ICO. It is therefore the responsibility of the Trust to ensure that the recommendations of the Data Protection Officer have been applied in terms of having policies in place and staff trained.

What is the Process? (please see Appendix 1)

Any incidents should be reported to the Trust Data Protection Officer (DPO) as soon as possible.

The member of staff who has identified the incident should complete and submit the on-line Security Incident Reporting Form which is available on YourIG.

The Incident Reporting Form should include:

- Number and type of records that are involved
- Detailed description of the incident, including any technical information
- If sensitive information has been compromised
- Remedial action that has been taken

An evaluation and assessment of the situation will be conducted by the DPO taking into consideration the following points:

- Was there any sensitive information compromised?
- Is there likely to be any media interest?
- Do Trust board members need to be involved?
- Is there a safeguarding issue as a result of the breach?

Investigating/Managing the incident

Upon receipt of the completed security incident reporting form the YourIG Data Protection Officer service will make an assessment of the severity of the incident. Following the assessment they will discuss with you the outcome of the assessment and any actions that need to be taken by the Trust and whether the incident requires reporting to the ICO.

Reporting of ICT incidents

Anyone in Trust who suspects an incident has occurred or identifies a vulnerability that could become an incident if ignored, which involves the use of ICT, should report it to their ICT provider **immediately.**

Working with the Trust IT operational manager

Examples of incidents that should be reported to IT operational manager include;

- virus problems,
- unexpected pop-ups on computer screens,
- unexpected programs running on computers,
- spear phishing (targeted scam emails),
- web site problems,
- problems related to permissions on files,
- MIS data issues,
- unauthorised escalation of privileges (e.g. pupils or staff having admin level access when they shouldn't have),
- disposal of media concerns,
- lost or stolen media or computers that contain passwords,
- remote access issues.
- unauthorised access to the network or email accounts

Reporting of ICT incidents

It is recommended that these records are reviewed, as a minimum, on a bi-annual basis, and that the records are retained for a period of 60 months.

Data Breaches Log

To meet the Accountability principle under Article 5 of UK GDPR Trust's are recommended to maintain a data breaches log. This should include the following:

(1) the date of the data breach;

(2) the unique reference number given to the data breach (Asset reference number);

(3) the nature of the breach;

(4) mitigation actions to limit the impact and severity of the breach;

(5) whether an ICO assessment has been undertaken;

(6) the severity assessment given by YourIG DPO Service;

(7) whether the data breach is reportable to the ICO;

(8) and whether an incident form has been completed.

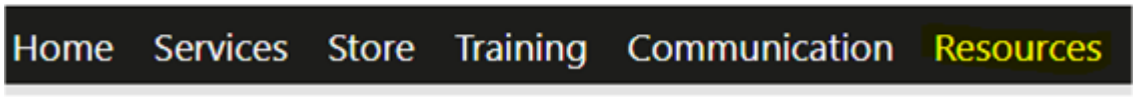
YourIG DPO Service has produced an excel spreadsheet for Trusts to use when logging a data breach. This should be reviewed on a regular basis to note any trends and lessons learned.

APPENDIX 1

Process of reporting a Security Incident

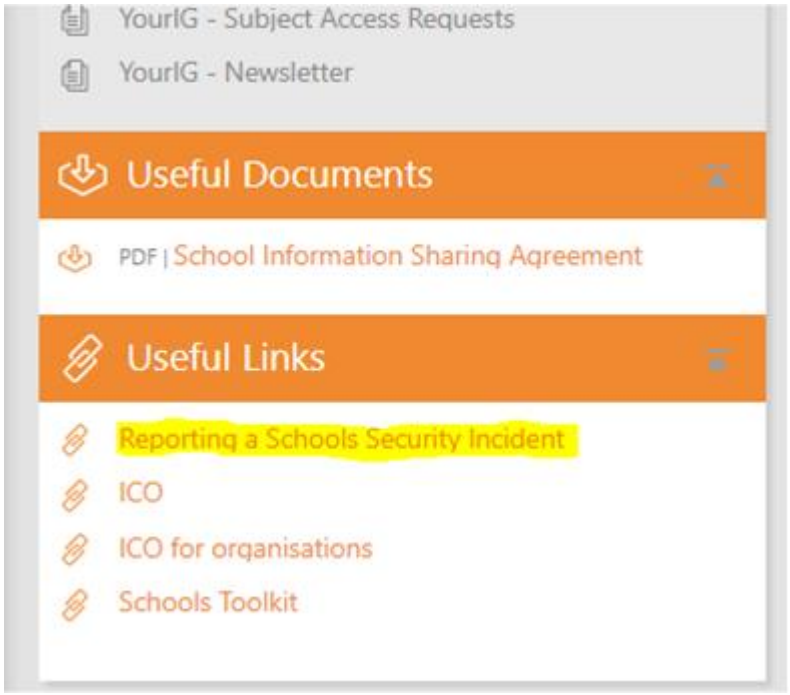
STEP 1: First log into the Revolution Portal.

STEP 2: Go to Resources on the main bar.



STEP 3: Browse the Resources list and find 'Information Governance and Data Protection Services' and click on the text to open the link.

STEP 4: On the right hand side under 'Menu' are two orange bars – under 'Useful Links' there will be a link for 'Reporting a Trusts Security Incident', click on this.



STEP 5: You'll then be presented with a form to fill in, if you can include as much information. This will generate a security incident reference (Assyst Number) which will come through to YourIG.

STEP: 6: YourIG will then ‘score’ the incident and rate it. This assessment will determine if the data breach needs reporting to the ICO.