William Torbitt Primary School

Data Security Breach policy

Policy Review

This policy was reviewed and adopted at the Governing Body Meeting in September 2019

This policy is due for review in June 2021

Contents

1 Background

Personal data breaches are increasingly common occurrences of Information Security Incidents whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached. Schools need to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect its information assets as far as possible.

Aim

The aim of this guidance is to standardise Schools responses to any reported data breach incident, and to ensure that they are appropriately logged and managed in accordance with best practice guidelines.

By adopting a standardised consistent approach to all reported incidents, the aim is to ensure that:

- Incidents are reported in a timely manner and can be properly investigated.
- Incidents are handled by appropriately authorised and skilled personnel
- Appropriate levels of School management are involved in response management.
- Incidents are recorded and documented.
- The impact of the incidents are understood and action is taken to prevent further damage
- Evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny.
- External bodies or data subjects are informed as required.
- The incidents are dealt with in a timely manner and normal operations restored
- The incidents are reviewed to identify improvements in policies and procedures.

Definition

A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Examples of data breaches can include:

- access by an unauthorised third party to confidential or highly confidential School Data
- Human error/sending personal data to an incorrect recipient;
- Equipment failure/computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceit

Near misses

A near miss is an event that does not result in a data breach, but which had the potential to do so. Examples of such events might include data that was misplaced but found quickly internally or data that was sent out but was identified and returned.

Your school should be committed to identifying weaknesses in your operational procedures. You will record all near misses in order to understand patterns, learn lessons and implement improvements.

If you come across any of the above and/or any other similar incidents, please follow the procedures for reporting an incident in the section below.

2 Information Security Incident Management and Reporting Procedure

The data breach procedure will involve the following 7 steps:

1. Containment and Recovery
2. Reporting the incident to the IT Team and Information Governance Lead
3. Risk Assessment
4. If necessary, notification to the ICO within 72 hours of becoming aware of the breach (Data Protection Officer/IG Manager to notify) and others who need to know e.g. Police, Suppliers, regulators etc.
5. Notification to the affected individuals, if required (If necessary)
6. Investigation of root cause analysis of the incident
7. Evaluation and learning from the incident e.g. amending processes/procedures, staff awareness

2.1 Containment and Recovery

Containing the incident and recovering the information (where possible) is crucial in the first instance, in order to recover from the impact of the incident.

Immediate safeguards should be taken where possible. For example, if email was sent to incorrect recipient by Egress revoke access via Egress, changing passwords, asking recipients to permanently delete the emails, taking information down from the website if unlawfully disclosed, asking IT or systems providers to restore data from backups collecting information sent by post to incorrect address, etc.

2.2 Reporting the incident

2.2.1 Reporting procedural Steps

At the earliest opportunity without undue delay (on the same day and no later than 24 hours), after having become aware of a personal data security breach/information security incident, report the ISI as follows:

i. if it is in relation to a lost item of technology (e.g. laptop, smart phone), or loss or breach of personal data notify the School IT Team and then submit in Information Security Incident Notification Form.

ii. if it is in relation to a loss or breach of personal data contact the Information Governance Lead and submit an Information Security Incident Notification Form as per point iv below.

iii. or contact the Information Governance Lead on Ext 88393, if you think it is a serious incident (e.g. lost papers, unauthorised/unlawful disclosure via email, post or verbal, a loss of usb stick that is not encrypted or the password is with it), and then submit **Error! Reference source not found.**an Information Security Incident Notification Form.

iv. Notify your line manager and if possible ask them to sign the notification form prior to submission. If this is not possible, then submit the form so that the risk to individuals affected can be immediately assessed in order to determine severity of the incident and whether it requires reporting to the ICO and then ask your line manager to sign the form.

email dataprotection.schoolsservicedesk@redbridge.gov.uk and submit an Information Security Incident Notification Form as soon as you can.

v. for incidents involving health and social care data please contact the Information Governance Lead immediately. They will determine whether the incident is a Security Incident Requiring Investigation in accordance with the guidance from the Health and Social Care Information Centre.

2.3 Risk Assessment

An immediate risk assessment will need to be carried out to establish the likelihood and severity of the actual or potential risk or negative consequence to the affected individuals. The results of this will need to be entered onto both the Notification Form and ISI Completion Form as appropriate.

This should be done quickly and where possible in consultation with the IG Lead.

In particular, where children or vulnerable people are affected, there may be other immediate actions you will need to take such as notifying the Police, carer's, home care provider, systems providers, foster carers, social worker etc. in order to contain or mitigate the actual or potential risks to them.

The Risk Assessment must consider the following -

1. The type of breach e.g. lost papers/device, email or letter sent to incorrect recipient, accidental disclosure, failure to redact, hacking or other cyber incidents etc.

2. Nature, sensitivity and volume of the personal data involved e.g. Health data, child protection data, bank details etc.

3. Ease of identification of individuals

4. Severity of consequences for individuals e.g. Could this breach lead to significant distress, financial or even physical harm? How likely is this to happen- very likely, likely, neutral- not likely or unlikely, unlikely etc. (See Appendix A)

5. Special characteristics of the individual e.g. Children, vulnerable person, person with a disability etc. Think about how this breach could cause these people harm.

6. Number of affected individuals

Categorise the incident in accordance with the severity in Appendix A. The Information Governance Lead can aid in this regard.

2.4 Notification to the ICO, and if necessary to others who need to know e.g. Police, Suppliers, regulators etc.

The GDPR requires data breaches or cyber incidents to be reported that is very likely or likely to cause actual or potential risk to individuals or is of sufficient concern and also any relevant authorities that need to know, such as the Police, carer's, systems providers, regulators etc.

In particular, where children or vulnerable people are affected, there may be other immediate actions you will need to take in order to contain or mitigate the actual or potential risks to them, such as notifying the social worker, foster carer or other partners involved with the child or the vulnerable person.

Following the risk assessment and determination of the severity of the incident/data breach the IG Lead will advise if the DPO is required to notify the ICO about the breach. If the DPO is required to notify the ICO this will need to be carried out within 72 hours of becoming aware of the breach. Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of the Schools turnover.

2.5 Notification to the affected individuals, if required

Where there is a very likely or actual or potential high risk to individuals, the GDPR requires organisations to notify the individuals affected. In the case of Pupils under the age of 16, this should be the Parent/Guardian or carer. This is should be carried out in a tactful way not to cause unnecessary distress.

You should consider, calling or visiting the individuals or Parent/Guardian or carer of the individuals affected where there is an actual or potential immediate high risk, harm or likely to have a significant effect on them for example, credit card details have been disclosed/compromised or the disclosure of the foster placement address of a child who is subject to a child protection plan etc. So that necessary steps, safeguards and actions can be taken by the individuals or people/third parries representing them. The Information Governance Lead can help you to determine whether a breach is of immediate high risk or harm.

In other cases where there is no immediate high risk or harm then they can be informed in writing.

2.6 Investigation and root cause analysis

The Line Manager of the staff member who notifies the Research and Data Team about the breach should lead and conduct an investigation on how the breach occurred. Where necessary they should engage the IG Lead, and their external suppliers or providers (if incident caused by supplier/service providers). The investigator should keep the IG Lead informed on progress of investigation

The investigator should keep all investigative activities documented including all actions and decisions taken and evidence supporting decisions and management of the risks and recovery of the information.

2.7 Evaluation and learning from the incident e.g. amending processes/ procedures, staff awareness

The investigator should evaluate the cause of the breach and effectiveness of response – and learn from mistakes. The Line Manager should ensure any gaps or weaknesses identified are rectified and appropriate measures and actions are implemented and incorporated into daily practice to prevent recurrence such as amending processes, procedures, additional staff training and awareness, regular spot checks or monitoring, fixing system errors or security controls etc.

The Information Security Incident Completion form should be filled in with all of the above information and signed by a Line Manager and sent to the Research and Data Team to ensure that a thorough management and investigation of the incident has been completed.

3 Health & Social Care Data

In the event of an incident involving health & social care data, a points-based system is to be used to determine whether notification via the reporting tool is necessary. Where the incident is at Level 2 or above, the expectation will be to report. The Information Governance Lead will make this determination based on the information in the notification form and any further investigation that they feel is required.

4 Reporting and Monitoring

All Information Security Incidents, including near misses, will be recorded on the data Information Security Breach Log by the Research and Data Team. All issues identified by the application of this policy will be recorded in the data breach log and categorised according to whether it is a data breach or near miss.

This information will be reviewed and analysed at least monthly to identify patterns and monitor the implementation of agreed service improvements.

The DPO will collate all data breach reports. The Information Governance Lead will report trends and lessons learnt to schools.

5 Non-Compliance

Non-compliance with this procedure could have a significant effect on the efficient operation of the School and may result in financial loss (up to €20 million euros or 4% of the school's annual turnover), reputational damage and an inability to provide necessary services to the public.

Staff who do not report data security breaches, or are found to be in breach of this procedure (e.g. failing to report a security incident) may be subject to the School's disciplinary process, which may in serious cases lead to dismissal.

APPENDIX A: Categorisation of Security Incidents

Incidents are categorised using three variables defined below.

Event (LOSS, DISCLOSURE, ACCESS, CONFIGURATION, DISRUPTION, USAGE)
Intent (MALICIOUS, MISUSE, THEFT/LOSS, ACCIDENTAL)
Impact (CRITICAL, SIGNIFICANT, MINOR, NEGLIGIBLE)

Examples:

- The theft of a child protection file from a locked car would be LOSS THEFT CRITICAL

- An unsuccessful virus attack would be DISRUPTION MALICIOUS MINOR

- An email being sent to the wrong place with basic personal information would be DISCLOSURE ACCIDENTAL SIGNIFICANT

Where appropriate, examples have been used to identify possible incidents, though this list is not exhaustive.

Event

An Information Security incident includes, but is not restricted to, the following *events*:

- The loss or theft of data or information. **(LOSS)**
- The transfer of data or information to those who are not entitled to receive it (**DISCLOSURE**)
- Attempts (either failed or successful) to gain unauthorised access to data or information stored on a computer system. **(ACCESS)**
- Changes to information or data or system hardware, firmware, or software characteristics without the School's knowledge, instruction, or consent. (**CONFIGURATION**)
- Unwanted disruption or denial of service to a system. **(DISRUPTION)**
- The unauthorised use of a system for the processing or storage of data by any person. **(USAGE)**

Intent

Malicious

- Giving protectively marked or personal, sensitive information to someone who you know should not have access to it - verbally, in writing or electronically.
- Computers infected by a virus or other malicious software (refer to the Virus Prevention Policy published on the intranet)
- Forwarding unsolicited e-mail / mail that require users to enter personal data.
- Unauthorised changes to information or data files.
- Forwarding chain e-mail – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Unknown people asking for information, which could help them to gain access to School information / data assets (e.g. a password or details of a third party).
- Deliberate, accidental disruption or denial of service to a computer or network system.
- Bogus personnel such e.g. someone pretending to be an engineer or contractor accessing, tampering with or taking computer assets away from School premises.
- Unauthorised changes to system hardware, firmware, and software characteristics without the School's knowledge, instruction or consent.

Misuse

- Use of unapproved or unlicensed software on School computer equipment
- Accessing a computer database using someone else's credentials e.g. user account and password.
- Password(s) and logon names written down and left on display.
- Printing or copying protectively marked information and storing it inappropriately.
- The unauthorised use of a computer or network system for the processing or storage of data by any person.
- Access details to restricted systems shared with others
- Sensitive documents disposed incorrectly
- Unauthorised information sharing
- Sending an email containing confidential information knowingly to ones personal email account or to another email address which is not the intended recipient.
- Discussing service users or customers with unauthorised third parties

Theft / loss

- Theft/loss of manual (paper) file.
- Theft/loss of portable data storage media e.g. USB devices, CDs, DVDs, backup tapes.
- Theft / loss of any School computer equipment e.g. laptop, PDAs, smart phones.
- Theft/loss of sensitive data processing assets e.g. payment card processing equipment.
- Theft/loss of sensitive information such as passwords, door codes, PINs, cryptographic information e.g. Cryptographic keys, PAN's (Primary Account Numbers).
- Theft/loss from your home, car etc. of any media containing School information e.g. a paper file, computer etc.

Accidental

- Sending an email containing confidential information unknowingly to an email address which is not the intended recipient.
- Accidental disclosure (unknowingly) verbally or electronically

The above list is not exhaustive. If you suspect an information security incident, see the Reporting Section above.

Impact

Impact Level	Description
Critical	**Cyber incident** These incidents will usually cause the degradation of vital service(s) for a large number of users, involve a serious breach of network security, affect mission-critical equipment or services, or damage public confidence in the government. **Personal Data Breach** **Incidents where sensitive/special categories of personal data (as defined by the General Data Protection Regulation) relating to more than one individual has been lost/stolen or disclosed to an unauthorised party will be regarded as critical.** **This includes where information has been emailed to unauthorised parties, has been physically lost (even if subsequently recovered), where the incident presents a very likely or high risk to individuals' rights and freedoms.** E.g. highly sensitive/child protection or DV information sent to the perpetrator, bank details hacked or published, targeted attacks or loss of publicly available online service. This category is reportable to the ICO and also to the individuals affected.
Significant	**Cyber incident** Less serious events are likely to impact a smaller group of users, disrupt non-essential services, breach network security policy, or affect the respect of government bodies and services. **Personal Data Breach** **Incidents where personal data and sensitive/special categories of personal data as defined by the General Data Protection Regulation or OFFICIAL or OFFICIAL-SENSITIVE DATA, will be regarded as significant where the incident presents a likely risk to individuals' rights and freedoms.** E.g. sensitive information sent to unauthorised recipient, website defacement or damaging unauthorised changes to a system, information containing a large volume of personal data or containing sensitive personal data relating one individual sent to an incorrect external recipient This category is reportable to the ICO**.**
Minor	**Cyber incident** Many types of incidents can be capably handled by local IT support, IG Manager and security officers and do not require National Cyber Security (NCSC) assistance, although NCSC should be notified of their occurrence. This aids the correlation of similar events, furthers the understanding of the IT security challenges facing government and may raise awareness of new attacks. **Personal data breach** **Incidents where personal data as defined by the General Data Protection Regulation or OFFICIAL DATA will be regarded as MINOR where the incident is unlikely to present risk to individuals' rights and freedoms.**

	E.g. This would be a near miss incident such as Egress emails successfully revoked, certain internal breaches where it has been contained, unsuccessful denial-of-service attack or the majority of network monitoring alerts. This category is not reportable to the ICO**.**
Negligible Impact	**Cyber Incident** It is not necessary to report on incidents of limited impact or those affecting only a few users. This sort of event would include receipt of isolated spam or anti-virus alerts, minor computer hardware failure, loss of network connectivity to a peripheral device such as a printer, or loss of access to an external non-essential service. In general these would be considered to be part of normal IT support operations. E.g. isolated anti-virus alert or spam email. **Personal data breach** Although there has been an incident but no personal data was compromised or lost. This category is not reportable to the ICO**.**

Personal data

'Personal data' is defined under the General Data Protection Regulation (GDPR) as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Sensitive or Special Categories of personal data

'Special categories of personal data' is defined under GDPR as personal data revealing;

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership, and
- the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,
- data concerning health
- data concerning a natural person's sex life
- sexual orientation
- criminal convictions and offences.

OFFICIAL-SENSITIVE marked information
This includes sensitive personal data but may also include contractual or legal information that would prejudice a negotiation if it was exposed inappropriately.

Please refer to the Information Security Policy Framework and Guidance on Handling Classified Information for the School Classification Policy.