Schools Personal Data Breach Procedure

Amended by:	Cathy Smart
Date agreed by Headteacher/Governing Body:	September 2019
Next review date:	September 2020

Schools Personal Data Breach Procedure Information Security Incident Reporting Policy and Procedures

Contents

1. INTRODUCTION

The Potton Federation processes personal data including special category personal data daily and it is essential that procedures are in place to ensure any threat to the security of that information is minimised and any breaches of the duties in respect of that information are identified and remedied. Any incident that compromises the security of that information, or the ICT system on which it resides, must be managed appropriately and in accordance with legislation and guidance provided by the Information Commissioners Office (ICO).

2. PURPOSE

The purpose of this policy is to ensure that the Federation reacts appropriately to mitigate the risks associated with actual or suspected security incidents relating to information systems and data. The Federation recognises that there are risks associated with users accessing and handling information to conduct official School business.

This policy aims to mitigate the following risks:

- Reduce the impact of information security incidents by ensuring they are followed up correctly
- Improve compliance by ensuring serious security incidents are reported to the appropriate external organisations
- To help identify areas for improvement to decrease the risk and impact of future incidents.

3. SCOPE

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the school. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. Under the GDPR, personal data' means 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.

This policy applies to all staff employed by our school, Governors and to external organisations or individuals working on our behalf.

All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of the School's systems and the information that they use or manipulate.
All users have a role to play and a contribution to make to the safe and secure use of information and communications technology, and the information that it processes or stores.

You must read, understand and comply with this Policy. This policy sets out what we expect from you in order for the School to comply with applicable law. Your compliance with this policy is mandatory. You must also comply with all related Policies and guidelines given. Staff who do not comply with this policy may face disciplinary action.

4. OBJECTIVES

The main objective of this policy is to ensure security incidents relating to School information and ICT systems are reported, recorded and investigated in accordance with the School's and legislative standards.

5. LEGAL REQUIREMENTS

As data controller personal data collected about staff, pupils, parents, governors, visitors and other individuals that is collected and held must be protected from unlawful misuse, loss, theft, accidental disclosure, destruction, corruption or alternation in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) as is currently set out in the Data Protection Bill.
This policy applies to all personal data, regardless of whether it is in paper or electronic format.

6. COMPLIANCE

If any user is found to have breached this policy, they may be subject to the Federation's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).
Non-compliance with this policy could have a significant effect on the efficient operation of the School and may result in significant financial loss.
The General Data Protection Regulation (GDPR) introduces a duty for us to report personal data breaches which are significant to the Information Commissioner. This must be done within 72 hours of the breach, where feasible.
If the breach is expected to adversely impact (or has a high likelihood of impacting) individual's rights and freedoms, we must also inform those individuals 'without undue delay'.
We will keep a record of any personal data breaches, regardless of whether we are required to notify.

7. DEFINITION

A personal data breach is more than just losing personal data. It is a breach of security leading to the accidental or lawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This policy needs to be applied as soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Examples of the most common personal data breaches and information security incidents are listed below. It should be noted that this list is not exhaustive.

- Giving information to someone who should not have access to it – this could be verbally, in writing or electronically.
- Theft / loss of a confidential paper
- Sending personal data to an incorrect recipient .e.g. groups of recipients such as ‘all staff' by mistake.
- Sending a text message containing personal data to all parents by mistake.
- Writing down your password and leaving it on display or somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially
- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- Computer infected by a Virus or other malware.
- Finding data that has been changed by an unauthorised person.
- Use of unapproved or unlicensed software on School ICT equipment.
- Accessing a computer database using someone else's authorisation (e.g. someone else's user ID and password).
- Changes to information or data or system hardware, firmware, or software characteristics without the School's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person

8. PROCEDURE FOR PERSONAL DATA BREACH AND SECURITY INCIDENT HANDLING

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact The School Business Manager who is the person designated as the key point of contact for Personal Data Breaches. You should preserve all evidence relating to the potential Personal Data Breach.

On finding or causing a breach, or potential breach, The School Business Manager must immediately notify the Data Protection Officer and take immediate remedial steps to mitigate and remedy the breach that has occurred. All reasonable steps must be taken to retrieve any information that has been unlawfully disclosed.
The DPO will provide advice on the immediate steps to be taken, investigate the report, and determine whether a breach has occurred.
The DPO will alert the Head teacher and the chair of governors if not already notified.
The DPO will assist The School Business Manager and relevant staff members or data processors where necessary to mitigate risk and impact.
The actions to be taken will be relevant to specific data types. The actions to minimise the impact of data breaches are set out below. These must, where relevant, be taken to mitigate the impact of different types of data breach. Breaches involving particularly risky or sensitive information must be acted upon swiftly and steps followed through.

The Potton Federation will review the effectiveness of these actions and amend them as necessary after any data breach.

EXAMPLE:
If sensitive information has been disclosed via email (including safeguarding records) or other special category data (sensitive information) such as health information is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error. Where this is unsuccessful or not possible immediate steps should be taken to contact the recipient with instructions to them to delete the email. If the sender is unavailable or cannot recall the email for any reason, the School Business Manager will ask the ICT department to recall it.
Where members of staff receive personal data sent in error they must alert the sender and School Business Manager as soon as they become aware of the error.
In any cases where the recall is unsuccessful, The School Business Manager will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way. The School Business Manager will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
The School Business Manager will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

INVESTIGATION AND REPORT

The DPO will carry out an internet search to check that the information has not been made public, if it has; we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO WITHIN 72 hours of the personal data breach coming to the attention of The School Business Manager.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

REPORT

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored securely in the School Business Managers Offices.

REVIEW AND PLANNING

The DPO and Headteacher will meet to review what happened and how it can be prevented from happening again. This meeting will happen as soon as reasonably possible. A report of data protection breaches and information security incidents will be presented to the Governing Board.

9. REPORTING INFORMATION SECURITY WEAKNESSES FOR ALL EMPLOYEES

Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such action may be considered to be misuse of information assets.
Weaknesses reported to third party application and service providers by employees must also be reported internally to the Schools ICT. The provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded and reported.
Security events can include:

- Uncontrolled system changes
- Access violations – e.g. password sharing
- Breaches of physical security
- Non-compliance with policies
- Repeated lock out of user accounts
- Flooding of the system with emails
- Malicious software (virus infections)
- Unscheduled shutdowns, system errors or overloads Security weaknesses can include:
- Inadequate firewall or antivirus protection
- System malfunctions or overloads

- Malfunctions of software applications
- Human error

All events must be logged with ICT and reported to The School Business Manager. A risk impact assessment must be carried out, and mitigation action including implementation timeframes identified.

10. REVIEW AND MONITORING ARRANGEMENTS

This policy will be reviewed and updated as and when necessary e.g. when the Data Protection Bill becomes law the Data Protection Act 2018. The DPO will review this policy at every annual audit and report any necessary changes to the Governing Body.

Further specialist information and advice may be sought from the Schools Data Protection Officer (see details below):

Cathy Smart

The Potton Federation

Mill Lane

Potton

Bedfordshire

SG19 2PG