# Data Protection Breach Procedure

## 1. Policy Statement

This policy should be read in conjunction with the Data Protection Policy. This policy has been written to deal with a data security breach. My Schools Together have taken appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

A data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.
- Equipment failure;
- Human error;

The personal data that we collect and process is limited. The Data Protection Information Audit lists the personal data we hold, what data is processed, where and how it is stored. Also, the audit has identified the risks associated with the data and the security measures in place to help minimise the risks.



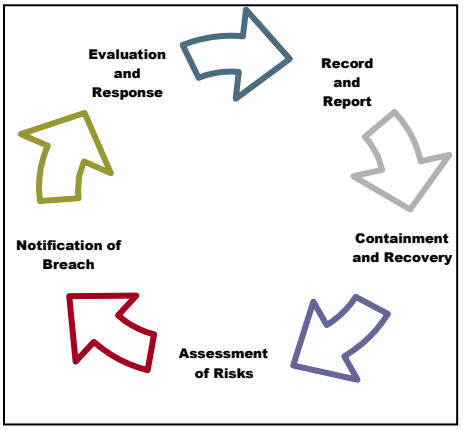
## 2. Responsibilities

This procedure applies to all My Schools Together employees, should a breach occur employees are required to inform a member of the SLT immediately and to share all relevant information regarding the breach

The SLT will implement the 5 actions listed below to help to manage the breach accordingly.

**Data Breach Procedure**

1. Record and Report
2. Containment and Recovery
3. Assessment of Risks
4. Notification of Breach
5. Evaluation and Response



## 3. Data Protection Breach procedure - 5 stages

### Stage 1: Record and Report

All data protection breaches must be recorded on the Data Protection Breach Reporting Form. The form helps to gather the information and to understand the impact of the incident and to help identify what must be done to reduce any risk to the organisation and person involved.

### Stage 2: Containment and Recovery

All data protection breaches will require an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of backup files to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.

### Stage 3: Assessment of Risks

Some data protection breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. While some incidents can still have significant consequences the risks are very different from those posed by, for example, the theft of a customer database, the data on which may be used to commit identity fraud.

Before deciding on what steps are necessary further to immediate containment, assess the risks which may be associated with the breach. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen. The following points will be helpful in making this assessment:

- What type of data is involved? How sensitive is it? Some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details). If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk. Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide? If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

# Data Protection Breach Procedure

## Stage 4: Notification of Breach

Informing people and organisations that you have experienced a data security breach can be an important element in the breach management procedure.

However, informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, to provide advice and deal with complaints.

The directors will consider who to notify, what they are going to tell them and how to communicate the message, this will depend to a large extent on the nature of the breach but the following points may be relevant to the decision:

- There are a number of different ways to notify those affected, we will consider the security of the medium as well as the urgency of the situation when making the decision;
- We will include a description of how and when the breach occurred , what data was involved and details of what has already done to respond to the risks posed by the breach;
- When notifying individuals we will give specific and clear advice on the steps they can take to protect themselves and also what we are willing to do to help them;
- We will also consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions - if applicable.

## Stage 5: Evaluation and Response

We will investigate the causes of the breach and evaluate the effectiveness of our response to it. If we identify where improvements can be made, then these improvements will be implemented.

All relevant information relating to a data protection breach and the findings from the investigation will be documented in the data protection breach reporting form.

## Data Protection Breach - Reporting Form

Person completing this form | Date

| Summary of Incident | |
|---|---|
| Date and Time of Incident | |
| Number of people whose data is affected | |
| Nature of breach e.g. theft/disclosed in error/technical problems | |
| Description of how breach occurred | |
| **Reporting** | |
| When was breach reported? | |
| How you became aware of the breach: | |
| **Personal Data** | |
| Full description of personal data involved (without identifiers); | |
| Number of individuals affected: | |
| Have all affected individuals been informed: | |
| If not, state why not: | |
| Is there any evidence to date that the personal data involved in this incident has been inappropriately processed or further disclosed? If so, please provide details: | |

# Data Protection Breach Procedure

| | |
|---|---|
| **Data Retrieval** | |
| What immediate remedial action was taken: | |
| Has the data been retrieved or deleted? If yes - date and time: | |
| **Impact** | |
| Describe the risk of harm to the individual as a result of this incident: | |
| Describe the risk of identity fraud as a result of this incident: | |
| Have you received a formal complaint from any individual affected by this breach? If so, provide details: | |
| **Management** | |
| Do you consider the employee(s) involved has breached information governances policies and procedures: | |
| Please inform of any disciplinary action taken in relation to the employee(s) involved: | |
| Had the employee(s) completed data protection training: | |
| As a result of this incident, do you consider whether any other personal data held may be exposed to similar vulnerabilities? If so, what steps have been taken to address this: | |
| Has there been any media coverage of the incident? If so, please provide details | |
| What further action has been taken to minimise the possibility of a repeat of such an incident? Please provide copies of any internal correspondence regarding any changes in procedure: | |