Botanic
PRIMARY SCHOOL

# Data Breach Management Procedure

May 2018

# Data Breach Management Procedure

Botanic Primary School is responsible for protecting the information it holds and is legally required under the General Data Protection Regulation (GDPR) to ensure the security and confidentiality of personal information processed.

## 1. 1. Policy statement

1.1. Every care is taken to protect information and to avoid a security incident, especially where the result is a data breach when personal information is lost or disclosed inappropriately to an unauthorised person. In the unlikely event of such a security incident, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. We will investigate all security incidents classified as serious using a set plan and follow a Breach Management Plan in the event of a data breach.

1.2. This Security and Data Protection Incident Reporting and Management Policy is in line with the current Information Commissioner's Office (ICO) guidance for reporting, managing and investigating breaches of personal data.

1.3. Botanic Primary School takes information security very seriously. Botanic Primary School understands the necessity to take prompt action in the event of any actual or suspected breaches of information security or confidentiality to avoid the risk of harm to individuals, damage to operational business and severe financial, legal and reputational costs to the school/MAT.

1.4. The GDPR introduces a mandatory requirement to report certain types of personal data breaches, which are likely to result in a risk to the rights and freedoms of individuals, to the Information Commissioner's Officer (ICO). The implementation of this Policy will ensure that personal data breaches are thoroughly investigated, with adequate remedial actions put in place and breach notification requirements complied with. In each case, specific GDPR provisions will be followed in a timely manner and within the specified timeframes.

1.5. GDPR Article 33(1): 'In the case of a personal data breach, the controller shall, without undue delay, and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.'

1.6. Botanic Primary School understands the severity of a failure to notify a reportable incident to the ICO. Failure to notify may lead to an administrative fine up to £500 000 or in case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

## 2. Objective

2.1. The objective of this Policy is to support the prompt and consistent management of information security incidents to minimise any harm to individuals such as pupils, parents and staff or the organisation.

2.2. This Policy supports the strategic business aims and objectives of Botanic Primary School by:

- ensuring that Botanic Primary School has implemented an effective information incident management and response mechanism that supports the implementation and sharing of lessons learned
- ensuring that there is a considered and agreed incident response and communications plan available, including the reporting of 'perceived' or 'actual' breaches
- ensuring that the investigation and reporting of data protection incidents conform to GDPR requirements and do not conflict with the organisation's policies and procedures
- facilitating the analysis of incident records to determine common risk patterns to raise awareness and implement preventative measures
- ensuring that every member of staff at Botanic Primary School understands the importance of reporting and managing information security incidents to reduce the risk of a future breach and to mitigate the impact of any potential breach.

## 3. Purpose

3.1. This Policy provides a framework for reporting and managing:

- security incidents affecting Botanic Primary School's information and IT systems
- losses of information
- near misses and information security concerns.

3.2. Everyone has an important part to play in reporting and managing information security incidents in order to mitigate the consequences and reduce the risk of future breaches of security.

## 4. General definitions

| TERM | DEFINITION |
|---|---|
| DATA CONTROLLER | A natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. |
| DATA PROCESSORS | A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller. |
| DATA PROTECTION | The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction. |

| | |
|---|---|
| DATA SUBJECT | Anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| ENCRYPTION | The process of encoding a message or information in such a way that only authorised parties can access it. |
| INFORMATION COMMISSIONER'S OFFICE (ICO) | An independent Public Authority in the UK responsible for monitoring the application of the relevant Data Protection regulation set forth in national law. |
| PERSONAL DATA BREACH | 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. |
| PROCESS, PROCESSED, PROCESSING | Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |

# 5. Scope

5.1. An information security incident is any event that has the potential to affect the confidentiality, integrity or availability of information in any format. Examples of a Personal Data Breach include the following (please note, this is not an exhaustive list):

- the loss or theft of data or information
- unlawful disclosure or misuse of confidential data/the disclosure of confidential information to unauthorised individuals
- using personal data in a way incompatible with the originally specified purpose
- information security breaches and inappropriate invasion of people's privacy
- personal data breaches which could lead to identity fraud or have other significant impact on individuals
- inappropriate access controls leading to unauthorised use
- any incident which involves actual or potential failure to meet the requirements of the GDPR and/or the common law of confidentiality
- loss or theft of paper records, data or equipment such as tablets, laptops and smartphones on which data is stored
- inappropriate access controls allowing unauthorised use of information
- attempts to gain unauthorised access to computer systems e.g. hacking
- virus or other security attacks on IT equipment systems or networks
- 'blagging offence, where information is obtained by deception
- breaches of physical security e.g. forcing of doors or windows into secure room, or filing cabinet containing confidential information left unlocked in accessible area

- leaving IT equipment unattended when logged in to a user account without locking the screen to stop others accessing information.

5.2. The Policy applies to all users of Botanic Primary School information. Users include all employees (including temporary workers), suppliers and visitors who may have access to Botanic Primary School information. All users must understand and adopt this Policy and are responsible for ensuring the safety and security of Botanic Primary School systems and the information that they use or manipulate. This includes both data stored electronically and in any other form.

# 6. Security of information

6.1. The new GDPR principle of accountability requires the Data Controller to be responsible for and to be able to 'demonstrate' and 'evidence' compliance with the Data Protection Principles.

6.2. Botanic Primary School is committed to putting in place adequate technical and organisational safeguards to prevent information security incidents and to establish immediately whether a breach has taken place. Technical safeguards can be thought of as physical protection ranging from ICT passwords and firewalls to building security, while organisational safeguards are aimed at employees (e.g. ensuring adequate training, policies and procedures are in place).

6.3. An Incident can be caused by a number of factors, such as:

- negligence or human error
- unauthorised or inappropriate access, including processing confidential personal data without a legal basis
- loss or theft of information or equipment on which information is stored
- systems or equipment failure
- accidents
- unforeseen circumstances such as fire, flood and other environmental factors
- inappropriate access, viewing information for purposes other than specified/authorised, e.g. an individual browsing a record about an ex-partner to find their current address
- unauthorised access, using other people's user IDs and passwords
- poor physical security
- inappropriate access controls allowing unauthorised use
- lack of training and awareness
- hacking attacks
- 'blagging' offences, where information is obtained by deception.

# 7. Procedure for incident handling

7.1. Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by the [insert name of responsible manager or team/group function].

## 7.2. Suspected Cyber Attack

7.2.1. Security events, for example a virus infection found within a malicious email attachment, could quickly spread and cause data loss across the organisation. All users must understand, and be able to identify, that any unexpected or unusual behaviour on the workstation could potentially be a software malfunction. If an event is detected users must:

- note the symptoms and any error messages on screen
- disconnect the workstation from the network if an infection is suspected (with assistance from the relevant staff member responsible for ICT in the school
- not use any removable media (for example USB memory sticks) that may also have been infected.

7.3. All suspected security events should be reported immediately to the ICT Co-ordinator and Principal

7.4. The ICT Co-ordinator will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- contact name and contact number of person reporting the incident
- the type of data, information or equipment involved
- whether the loss of the data puts any person or other data at risk
- location of the incident
- inventory numbers of any equipment affected
- date and time the security incident occurred
- location of data or equipment affected
- type and circumstances of the incident.

## 7.5. Other Incidents

7.5.1. If the Information Security event is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported to the Principal.

## 7.6. Collection of Evidence

7.6.1. If an incident may require information to be collected for an investigation, strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care.

# Breach management plan

There are four important elements to any breach management plan:

1. Containment and recovery
2. Assessment of ongoing risk
3. Breach notification
4. Evaluation and response

## 1. Containment and recovery

Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the school, such as ICT, HR and legal and, in some cases, contact with external stakeholders and suppliers.

Consider the following:

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.
- 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. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.
- 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 back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Where appropriate, inform the police where there is evidence to indicate a crime has taken place.
- Where appropriate, consider reporting a personal data breach to the ICO.

## 2. Assessment of ongoing risks

Before deciding on what steps are necessary following immediate containment, assess the risks which may be associated with the breach. The following points are also likely to be helpful in making this assessment:

- What type of data is involved?
- How sensitive is it?
- If data has been lost or stolen, are there any protections in place such as encryption?
- Regardless of what has happened to the data, what could the data tell a third party about the individual?
- How many individuals' personal data are affected by the breach?
- 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?
- 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.

# 3. Breach notification

## 3.1. Mandatory reporting to the ICO

3.1.1. Under GDPR, Botanic Primary School is required to notify the ICO of a breach where it is likely to result in a 'high risk' to the rights and freedoms of individuals.

3.1.2. Whether there is such a risk is also likely to vary depending on the type of data that is the subject of the breach and the type of breach that has occurred. A breach that is likely to have a significant detrimental effect on individuals, e.g. disclosure of an individual's health or financial information, may be likely to have a significantly higher risk to the rights and freedoms of a data subject than a breach that leads to disclosure of individual's names with no further information about the individuals.

3.1.3. This must be assessed on a case-by-case basis. For example, you will need to notify the ICO about a loss of pupil/parent details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

3.1.4. The severity of the personal data breach/incident will be determined by the scale (numbers of data subjects affected) and sensitivity factors selected. If the outcome in terms of the severity of the incident is Level 2 (reportable), the incident should be reported to the ICO and escalated to other regulators, as appropriate. Please refer to Annex A – Incident Severity Assessment, which will help determine whether an incident is externally reportable.

3.1.5. Although the primary factors for assessing the severity level are the numbers of individual data subjects affected, the potential for media interest, and the potential for reputational damage, other factors may indicate that a higher rating is warranted, for example the potential for litigation or significant distress or damage to the data subject(s) and other personal data breaches of the GDPR. As more information becomes available, the personal data breach should be re-assessed. Where the numbers of individuals that are potentially impacted by an incident are unknown, a sensible view of the likely worst case should inform the assessment of the incident. When more accurate information is determined, the level should be revised as quickly as possible.

Please note: No reporting is required if the breach is unlikely to result in a risk to the rights and freedoms of natural persons. For example, when lost data is protected, e.g. by appropriate encryption, so that no individual's data can be accessed, then there is no data breach. When the data is protected but risk of individuals being identified remains, an incident should be reported.

## 3.2. Timing

3.2.1. Where a personal data breach is deemed reportable to the ICO, it must be reported without undue delay and, where feasible, not later than 72 hours after becoming aware of it.

3.2.2. Where a notification is not made within 72 hours of the data breach, Botanic Primary School must give a 'reasoned justification' to the ICO explaining the reason for the delay.

3.2.3. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases. In practice, notification to the ICO may be required initially, followed by an in-depth analysis of the incident.

### 3.3. Communicating personal data breaches to individuals affected

3.3.1. If the breach is sufficiently serious to warrant notification to the public, Botanic Primary School will do so without undue delay.

3.3.2. Informing pupils, parents and staff that you have experienced a data security breach can be an important element in Botanic Primary School's breach management strategy. Considering the following will assist the organisation in deciding whether and how to notify:

- Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by being able to monitor any unusual or suspicious bank transactions, checking their credit rating, cancelling a credit card or changing a password?
- If a large number of people are affected, or there are very serious consequences, you should inform the ICO.
- Consider how notification can be made appropriate for particular groups of individuals, for example, if you are notifying children or vulnerable adults.
- Have you considered the dangers of 'over notifying'? Not every incident will warrant notification.
- You also need to consider who to notify, what you are going to tell them and how you are going to communicate the message. The notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to respond to the risks posed by the breach.
- When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them. For example, you may wish to pay for annual subscription to a credit reference agency where financial data may have been compromised.
- Provide a way in which they can contact you for further information or to ask you questions about what has occurred – this could be a helpline number or a web page, for example.

3.3.3. There are, however, some circumstances when the notification to the data subject is not required, including:

- Botanic Primary School has implemented appropriate technical and organisational protection measures in respect of the personal data affected by the breach (such as encryption).
- Botanic Primary School has taken subsequent measures which ensure that the high risk to the rights and freedoms of individuals is no longer likely to arise.
- It would involve disproportionate effort. A public notice or similar would be required to communicate the breach in those circumstances.

3.3.4. The ICO may compel Botanic Primary School to communicate a personal data breach with affected data subjects/individuals unless one of the three exemptions listed above is satisfied.

## 4. Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of your response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if your response was hampered by inadequate policies or a lack of a clear allocation of responsibility, then it is important to review and update these policies and lines of responsibility in light of the experience.

# Annex A

## 1. Incident severity assessment

1.1. Not all incidents have the same potential to adversely impact on the individuals whose data are involved. Assessing the severity of an incident relies on several factors, and there is no simple definition that covers what a serious incident entails. An incident that at first appears to be of minor importance may, on further investigation, be found to be serious and vice versa.

1.2. Although the full extent of an incident is only known after it has been thoroughly investigated, there is a need to ascertain whether the risk could be classified as serious at an early stage.

The crucial factors for assessing the severity level of an incident are:

- the number of individual data subjects (pupils, staff and parents) affected
- the potential for significant distress or damage to the data subject
- the potential for reputational damage to Botanic Primary School
- the potential for litigation
- the potential for media interest
- the type of personal data breach. Data breaches affecting special categories of data are more sensitive, and thus need to be treated more seriously than data breaches of personal data (refer to Appendix D for a complete list of what constitutes special categories of data).

1.3. Loss or theft of encrypted removable media (laptops, CDs, USB memory sticks, media cards, Personal Digital Assistants (PDAs)) would not constitute a reportable incident unless there is reason to believe that the protection afforded by these devices has been compromised, e.g. the key(s) used to unencrypt have also been compromised, the laptop was not configured to automatically enforce account lockout after a short time lapse without user interaction, or using an untested proprietary encryption algorithm.

1.4. There are two factors which influence the severity of an Information Governance Serious Incident Requiring Investigation (IG SIRI) – scale and sensitivity.

### 1.5. Scale factors

1.5.1. While any personal data breach is potentially a very serious matter, the number of individuals that might potentially suffer distress, harm or other detriment is clearly an important factor. The scale (as demonstrated in Table 1 below) provides the base categorisation level of an incident, which will be modified by a range of sensitivity factors.

### 1.1. Sensitivity factors

1.1.1. Sensitivity in this context may cover a wide range of different considerations and each incident may have a range of characteristics, some of which may raise the categorisation of an incident and some of which may lower it. The same incident may have characteristics that do both, potentially cancelling each other out. For the purpose of the incident, sensitivity factors may be:

- Low: Reduces the base categorisation
- High: Increases the base categorisation.

### 1.2. Categorising Personal Data Breaches

1.1.1. The incident category is determined by the context, scale and sensitivity. Every incident can be categorised as:

- Level 0 or 1: Confirmed incident but no need to report to ICO and other regulators.

- Level 2 or above: Confirmed incident that must be reported to ICO and other regulators.

1.2.1. To determine which category your incident falls under, first use Table 1 to identify the baseline category for the breach, based on the scale of the incident, then use Table 2 to determine the final category, based on the sensitivity of the incident.

| Baseline category | Definitions |
|---|---|
| 0 | Information about less than 10 individuals |
| 1 | Information about 11–50 individuals |
| 1 | Information about 51–100 individuals |
| 2 | Information about 101–300 individuals |
| 2 | Information about 301–500 individuals |
| 2 | Information about 501–1,000 individuals |
| 3 | Information about 1,001–5,000 individuals |
| 3 | Information about 5,001–10,000 individuals |
| 3 | Information about 10,001–100,000 individuals |
| 3 | Information about 100,001 + individuals |

Table 1: Baseline category based on scale of incident

| Scores | Sensitivity characteristics |
|---|---|
| +1 FOR EACH CHARACTERISTIC | Sensitive categories of data (Appendix D) |
| | Detailed information at risk, e.g. financial information |
| | One or more previous incidents of a similar type in past 12 months |
| | Failure to securely encrypt mobile technology or the other obvious security failing |
| | media interest |
| | A complaint has been made to the ICO |
| | Individuals affected have been placed at risk of physical harm |
| | Individuals affected may suffer significant detriment, e.g. financial loss |
| | Individuals affected are likely to suffer significant distress or embarrassment |
| -1 FOR EACH CHARACTERISTIC | No data at risk |
| | Limited demographic data at risk, e.g. address not included, name not included |
| | Security controls/ difficulty to access data partially mitigates risk |

Table 2 – Category changes based on sensitivity

| Final score | Level of incident |
|---|---|
| 1 OR LESS | Level 1 incident (to be reported internally) |
| 2 OR MORE | Level 2 incident (to be reported to the ICO, and internally) |

Table 3 – Incident reporting requirements

## 2. Notification of data breaches to the ICO

2.1. There are also prescribed requirements under the GDPR to satisfy when communicating a breach to the ICO. Guidance from the ICO regarding reporting of incidents is detailed in the list below and included in the Incident Report Form Template in Appendix B.

2.2. Information should include:

- Botanic Primary School contact details, stating Botanic Primary School is the Data Controller in respect of the data breach
- the Data Controller registration number, although under the GDPR this will no longer be a mandatory requirement
- contact details of person in charge of the incident: name, job title, email address, contact telephone number and postal address
- the reason(s) for any delay(s) in notifying, if applicable
- measures the organisation have in place to prevent an incident of this nature occurring
- extracts of relevant policies and procedures
- what personal data has been placed at risk
- number of individuals affected and approximate number of data records concerned
- whether the affected individuals have been made aware of this breach
- the potential adverse effects on those individuals
- any palliative measures taken
- whether the data placed at risk has been recovered
- evidence of existing staff training, including relevant excerpts, and whether it is mandatory
- any previous incidents that had been reported to the ICO, providing a succinct summary.

2.3. This information is to be sent to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

2.4. The ICO will issue an initial response within seven calendar days and provide a case reference number and information about their next steps.

2.5. Furthermore, Botanic Primary School has a duty to inform Data Subjects whether there is potential for identity theft which can be avoided or minimised if the Data Subject is notified of the incident, without undue delay.

2.6. Failing to comply with the notification requirement under the GDPR means Botanic Primary School will potentially attract GDPR fines, such as €20 million, or 4% of the company's annual global turnover, whichever is higher.

## 3. Incident management

3.1. An individual must be assigned to manage the incident, and will be responsible for communicating and coordinating activities, as well as maintaining an audit trail of events and evidence. An investigation needs to be conducted to determine the causes of the breach, the scope, and possible remediation, along with expected outcomes and the identification of stakeholders. Evidence is to be preserved in order of volatility.

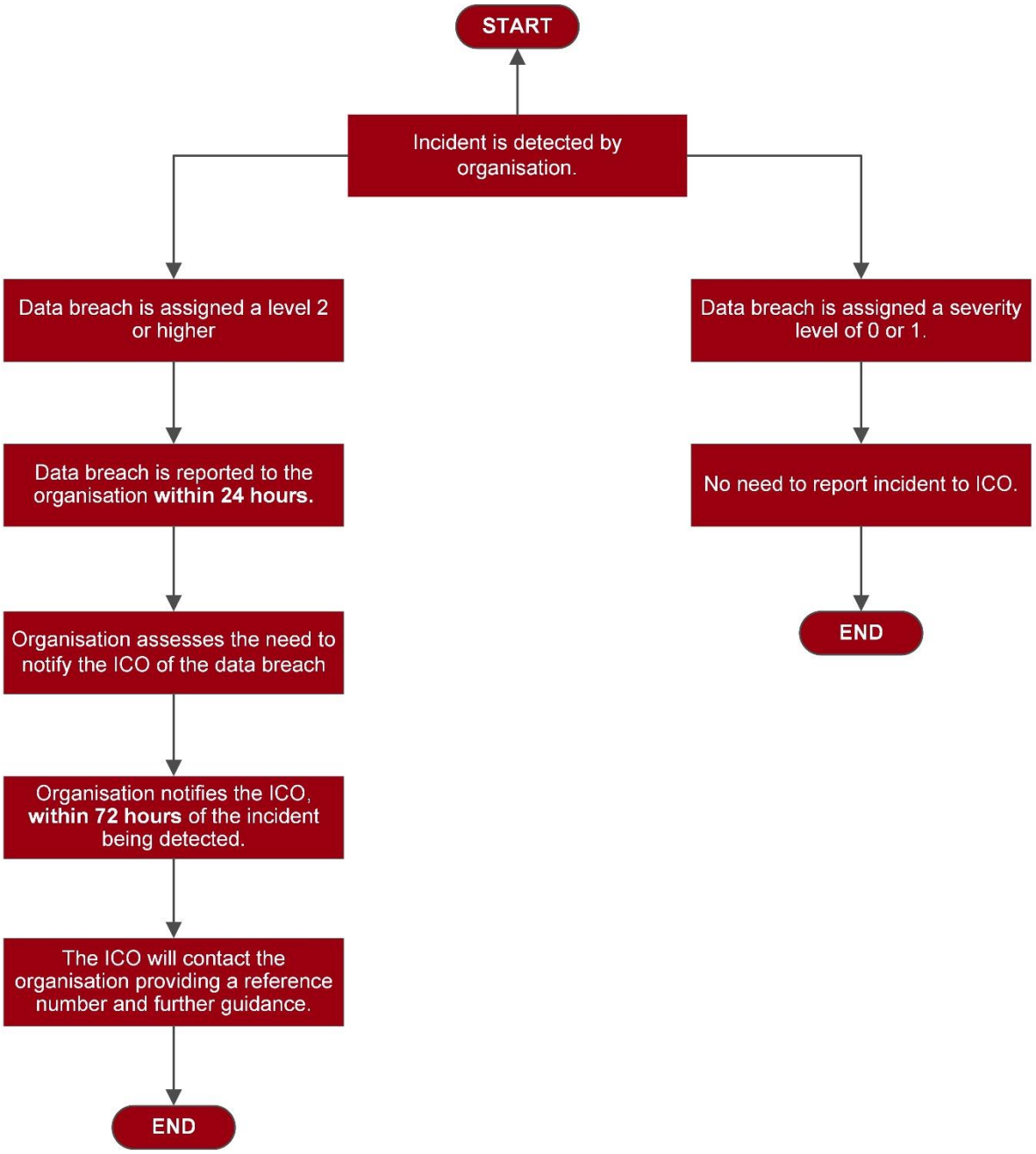
3.2. Following the investigation, mitigation and preventative measures must be documented and put in place, and a final incident report produced to obtain a sign-off from the Botanic Primary School board.

# 4. Personal data breach register

4.1. Under the GDPR, both Data Controllers and Data Processors are required to record any personal data breaches and any actions taken in respect of that. An Internal Breach Register will be maintained, documenting each incident 'comprising the facts relating to the personal data breach, its effects and the remedial action taken'.

4.2. The ICO has the authority to assess how Botanic Primary School complies with its data breach notification obligations.

# Appendix A – Incident management flow diagram



# Appendix B – ICO incident report template

| ICO INCIDENT REPORT FORM | | |
|---|---|---|
| Date | Time | Location |
| Organisation name | | |
| name of person reporting incident | | |
| Job title | | |
| Phone number | | |
| Postal address | | |
| Email address | | |
| Description of incident | | |
| Reason for delaying notification, if applicable | | |
| Number of people affected | | |
| Volume of data affected | | |
| Measures [Insert Organisation Name] has in place to deal with such incidents | | |
| Potential adverse effects on individuals affected | | |
| Mitigating measures taken | | |
| Have the data been recovered? | | |
| Has [Insert Organisation Name] reported data breaches to the ICO in the past? If yes, provide details. | | |

# Appendix C – Template to log and report incidents internally

| INTERNAL INCIDENT REPORT FORM | | |
|---|---|---|
| Date | Time | Location |
| name of person reporting incident | | |
| Job title | | |
| Phone number | | |
| Email address | | |
| Description of incident | | |
| Level of incident | | |
| Number of people affected | | |
| Volume of data affected | | |
| Data format (paper/electronic) | | |
| If electronic, are records encrypted? | | |
| Is the incident in the public domain? | | |
| Is the media aware of the incident? | | |
| Immediate action taken | | |
| Remedial action taken | | |
| For [Insert Organisation Name] use | | |
| Incident reference number | | |
| Received by | | |
| Forwarded for action to | | |
| Remedial action taken | | |

# Appendix D – Special categories of data

| |
|---|
| Racial or ethnic origin of the data subject |
| Political opinions |
| Religious beliefs or other beliefs of a similar nature |
| Trade union membership |
| Physical or mental health condition |
| Sexual life |
| The commission or alleged commission by the individual of any offence |
| Any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings |
| Biometric or genetic data |