Information Security Incident and Personal Data Breach Management Procedure

Procedure Reference:		G24a	
Related Policy:		G24	
Effective date:	March 2023	**Review date:**	March 2026
Approved by P&PRG:		February 2023	
Owner:	Lyn Docherty	**Job Title:**	Head of Compliance and Improvement
To be issued to:		All Staff	
Method of Delivery:		E-mail alert to new procedures with a summary of key points to be circulated by Data Protection Lead	

Version Control

Date	Owner	Version	Reason for Change
March 2023	**Lyn Docherty**	**1.0**	**New Procedure**

Summary of Changes

Section	Change
Whole procedure	Existing Ark procedure G48 reviewed and DPO advised that it should be separated in to individual procedures and updated

Information Security Incident and Personal Data Breach Management Procedure

Contents

1.0 Introduction

In today's world, information is constantly at risk of being involved in a security incident. Cyberattacks, ransomware, phishing, malware, system and process failure, staff mistakes, lost or stolen devices are examples of how data can be lost or compromised.

Ark is required to record all incidents that could result in a breach of the data protection regulations. Ark's Data Protection lead will maintain a register of incidents and whether these have resulted in personal data breaches for Ark.

A security incident, resulting in a breach could damage Ark's reputation and our relationship with our stakeholders or expose the organisation, our staff, supported people or tenants to the risk of fraud or identity theft. In addition, considerable distress could be caused to the individuals concerned, as a result of which, Ark could face legal action.

Some breaches must be reported to the Information Commissioners Office within 72 hours of Ark being made aware. There are also requirements to notify the individuals whose personal data has been involved in the breach, under certain circumstances. Consideration must also be given to whether the incident should be reported to the Scottish Housing Regulator as a notifiable event – see Ark's Notifiable Events Procedure [G50].

The Information Commissioners Office have the right to impose enforcement notices on Ark or monetary fines for breaches, including the failure to notify a breach.

2.0 What is a Security Incident?

An information security incident is a suspected, attempted, successful, or imminent threat of unauthorised access, use, disclosure, modification, or destruction of information; interference with information technology operations; or significant violation of our Privacy and Data Protection Policy (G24) or Computer System Security Email Internet Policy (G15).

Examples of information security incidents:

- Computer system intrusion
- Unauthorised access to premises where information is stored
- Unauthorised or inappropriate disclosure of organisation information
- Suspected or actual breaches, compromises, or other unauthorised access to Ark's systems, data, applications, or accounts
- Unauthorised changes to computers or software
- Loss or theft of computer equipment or other data storage devices and media (e.g., laptop, USB drive, personally owned device used for work) used to store or access Ark's information.
- An attack that prevents or impairs the authorised use of networks, systems, or applications
- Interference with the intended use or inappropriate or improper usage of information technology resources.

A Security Incident involving personal data is considered a Personal Data Breach. If a security incident does not involve personal data, it will still be logged and investigated under this procedure.

3.0 What is a Personal Data Breach?

A personal data breach is a security incident (as outlined above) leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It is important to understand that a personal data breach is more than just losing personal data.

Essentially while all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.

4.0 Roles and Responsibilities

4.1 All Ark Employees

All Ark personnel are required to:

- Report any security incidents to the Data Protection lead
- Assist with any investigation
- Implement any actions to contain and recover information

4.2 Data Protection Lead / Data Protection Officer

Ark's Data Protection Lead/Data Protection Officer will:

- Record all security incidents
- Decide if incident has resulted in a personal data breach
- Manage investigations and actions to contain and recover information
- Notify the relevant staff, ICO, data subjects
- Identify lessons learned and implement actions to reduce future re-occurrence.
- Ensure appropriate resources are allocated to assist in breach investigations, containment and recovery
- Review Breach Register and reports

5.0 Reporting a Security Incident

It is the responsibility of all personnel to report any suspected or actual security incident as soon as possible to Ark's Data Protection Lead at the latest the next working day. It is vital that the Data Protection Lead is notified of the incident promptly in order to ensure Ark takes all immediate actions available to reduce the impact of the incident, identify if personal data is involved and if notification is required to the Information Commissioners Office (ICO) or any relevant data subjects.

You should report any incident by telephoning Ark's Data Protection Lead and follow up with an email if you are unable to make direct contact via the phone.

Where an incident involves electronic data or IT systems, the Data Protection lead will notify the ICT and Head of ICT Strategy and Development as soon as possible.

6.0 Containment & Recovery

An Incident requires investigation promptly to contain the situation and allow the creation of a recovery plan including, where necessary, damage limitation. This will often involve input from across the organisation.

The following will be established:

- Who is required to investigate the breach with the DPO and what resources will be required
- 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.)
- Whether there is anything we can do to recover any losses and limit the damage the breach could 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 personnel recognise when someone tries to use stolen data to access accounts.)
- If criminal activity is suspected the Police will be informed.

7.0 Assessing the Risks

Some data security incidents will not lead to risks beyond possible inconvenience to those who need the data to do their job. For example, where a laptop is irreparably damaged, but its files were backed up and can be recovered, albeit at some cost to the business.

While these types of 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, the risks associated with the incident will be assessed. 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 will be used to make an assessment:

- What type of data is involved? If it includes personal data it will be considered a Personal Data Breach
- How sensitive is it? Remember that 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, could it be used for purposes which are harmful to the individuals to whom the data relate or the organisation; 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 an individual or the organisation? 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 or tenants, 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 individuals or the organisation? Are there risks to physical safety or reputation, of financial loss or a combination of these?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service we 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.

8.0 Notification

8.1 Notification to ICO

Ark has to notify the ICO (via the DPO) of a personal data breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed, such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination,

damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Incidents have to be assessed on a case by case basis. For example, we will need to notify the ICO about a loss of customer 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.

The decision to notify the ICO will be made by the Head of Compliance and Improvement and Ark's Data Protection Lead with advice from the DPO. A written record of this decision will be recorded in the Breach Register.

Appendix 1 provides examples of what breaches require notification and to whom.

8.2 Information to be provided to the ICO

- The nature of the personal data breach including, where possible: the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned.
- The name and contact details of the Data Protection Officer or other contact point where more information can be obtained.
- A description of the likely consequences of the personal data breach. A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

8.3 How to notify the ICO

A notifiable breach has to be reported to the ICO within 72 hours of us becoming 'aware' of it. When we become 'aware' of the breach is the point when we know or suspect there has been a personal data breach. We may not discover that a security incident is a personal data breach initially, but as soon as we do know or suspect that personal data is involved then we are 'aware'.

Some examples to help determine when we become aware:

- In the case of a loss of a USB Drive with unencrypted data it is often not possible to ascertain whether unauthorised persons gained access. Nevertheless, such a case has to be notified as there is a reasonable degree of certainty that a breach has occurred; we would become 'aware' when we realised the CD had been lost

- A third party informs us that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As we have been presented with clear evidence of a breach then there can be no doubt that we have become 'aware'
- We detect that there has been a possible intrusion into our network. We check our systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, we now have clear evidence of a breach there can be no doubt that we have become 'aware'

It is recognised that it will often be impossible to investigate a breach fully within the 72 hour time-period and legislation allows for us to provide information to the ICO in phases.

8.4 Delayed Notifications

If it is not possible to notify the ICO within 72 hours, when notification is completed it must include the reasons for the delay. We should always aim to notify the ICO as soon as possible even if we do not have much detail at that point.

8.5 Notification to Data Subjects

If the breach is sufficiently serious to warrant notification to the public, we must do so without undue delay.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we must notify those concerned directly and without undue delay, unless this would involve disproportionate effort.

If it is not possible to contact the data subjects directly or there is a large volume of data subjects involved, then we should make a public communication or similar measure whereby the data subjects are informed in an equally effective manner. Dedicated messages must be used when communicating a breach to data subjects and they should not be sent with other information, such as regular updates or newsletters. This helps to make the communication of the breach to be clear and transparent.

Examples of transparent communication methods include direct messaging (e.g. email, SMS), prominent website banners, social media posts or notification, postal communications and prominent advertisements in printed media.

Communicating a breach to data subjects allows us to provide information on the risks presented as a result of the breach and the steps the data subjects can take to protect themselves from its potential consequences.

8.6 Information to be provided to Data Subjects

We must provide the following information:

- A description of the nature of the breach
- The name and contact details of the Data Protection Officer or other contact point
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to be taken by us to address the breach, including, where appropriate, measures to mitigate its possible adverse effects

If the data subject wishes to raise a complaint about the breach, this should be escalated to the Data Protection Officer.

9.0 Evaluation

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of our response to it once completed.

If it was identified that 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. Also, if the management of the breach 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 the light of experience.

We may find that existing procedures could lead to another breach and we will need to identify where improvements can be made.

Ark's Data Protection Lead will work with the relevant staff involved in the breach to review process and procedures, to ensure that effective measures have been taken to prevent a recurrence of the breach and to monitor ongoing compliance.

The Data Protection Lead will publicise any identified learning outcomes to all parties who may benefit from the updated guidance or information.

10.0 Records Management

A Security Incident and Breach Register will be maintained by the Data Protection lead.

A case file will be made for each investigation to ensure a full record of the investigation, any correspondence, and decisions on notifications, are maintained accurately and retained as per the Ark Records Retention Schedule.

11.0 Implementation and Review

11.1 Implementation

The Operational Management Team (OMT) is responsible for ensuring that this procedure is implemented throughout the organisation.

11.2 Review

This procedure will be reviewed every 3 years or when required to address any weakness in the procedure or changes in legislation or best practice.

Appendix 1 - Notification Guidance

Examples of personal data breaches and who to notify. (Taken from Article 29 Working Group adopted guidance)

The following non-exhaustive examples will assist in determining whether we need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	**Notify the ICO**	**Notify the Data Subject(s)**	**Notes**
A controller stored a backup of an archive of personal data encrypted on a CD. The CD is stolen during a break-in	No	No	As long as the data are encrypted with a state of the art algorithm, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However, if it is later compromised, notification is required
Personal data of individuals are infiltrated from a secure website managed by the controller during a cyber-attack.	Yes, report to ICO if there are potential consequences to individuals	Yes, depending on the nature of the personal data affected and if the severity of the potential consequences to individuals is high	If the risk is not high, we recommend the controller to notify the data subject, depending on the circumstances of the case. For example, notification may not be required if there is a confidentiality breach for a newsletter related to a TV show, but notification may be required if this newsletter can lead to political point of view of the data subject being disclosed
A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No	No	This is not a notifiable personal data breach, but still a recordable incident. Appropriate records should be maintained by the controller
A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system	Yes, report to the ICO, if there are potential consequences to individuals as this is a loss of availability	Yes, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences	If there was a backup available and data could be restored in good time, this would not need to be reported to the ICO or to individuals as there would have been no permanent loss of availability or confidentiality. However, the ICO may consider an investigation to assess compliance with the broader security requirements
An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone	Yes	Only the individuals affected are notified if there is high risk and it	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and

else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and if it is a systemic flaw so that other individuals are or might be affected		is clear that others were not affected	the controller takes the additional step of notifying other individuals if there is high risk to them
Personal data of 5000 students are mistakenly sent to the wrong mailing list with 1000+ recipients	Yes	Yes, depending on the type of personal data involved and the severity of possible consequences	
A direct marketing e-mail is sent to recipients in “to:” or “cc:” field, thereby enabling each recipient to see the email address of other recipients	Yes, notifying the ICO may be obligatory if a large number of individuals are affected, if sensitive data are revealed	Yes, depending on the type of personal data involved and the severity of possible consequences	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.