Newable

Data Protection Breach Policy

Version 3.3

Version Control

Version	Owner	Reviewer	Changes	Approval date	Next Review
1.0	Joanne Wilkinson	Brendon Simpson	Initial version	04/2018	04/2019
2.0	Joanne Wilkinson	Gavin Holland	Annual review	08/2020	08/2022
3.0	Mashudul Karim	Gavin Holland	Updated names and terminology	03/2024	03/2025
3.1	Mashudul Karim	Gavin Holland	Clarified position of UK GDPR and UK DPA in Background.	03/2025	03/2026
3.2	Mashudul Karim	Gavin Holland	Corrected email address for DPO.	04/2025	03/2026
3.3	Mashudul Karim	Gavin Holland	Added references to DUAA	04/2026	04/2027

Contents

Background

The General Data Protection Regulation (GDPR) entered into force across the EU on 25 May 2018, replacing the EU Data Protection Act (DPA). Although the UK has formally withdrawn from the EU, it has incorporated the GDPR into domestic law as the UK GDPR and augmented it with the Data Protection Act 2018.

On 5 February 2026, significant changes to UK data protection law took effect under the Data Use and Access Act 2025 (DUAA).

All references to the GDPR and DPA in this document relate to the UK GDPR and the UK DPA as augmented by the DUAA.

Newable is responsible for protecting the information it holds, and it is legally required to hold under the GDPR, to ensure the security and confidentiality of personal information processed.

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

Newable takes information security very seriously. Newable 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 organisation.

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 ICO. Newable's Data Protection Officer (DPO), Mashudul Karim, will consult with and report breaches directly to the ICO. The implementation of this Policy will ensure that Newable thoroughly investigates personal data breaches, with adequate remedial actions put in place, complies with breach notification requirements.

In each case, Newable will follow specific GDPR provisions in a timely manner and within the specified times.

A data breach may comprise the following:

- a **confidentiality breach**, where there has been unauthorised or accidental disclosure of or access to personal data;
- an **integrity breach,** where there has been unauthorised or accidental alteration; or,
- an **availability breach,** where there has been accidental or unauthorised loss of access to or destruction of data (e.g., by a power cut or systems failure).

GDPR Article 33(1) states that *"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."

Newable 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 €20,000,000 or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding fiscal year, whichever is higher.

Objectives

The objective of this Policy is to support the prompt and consistent management of information security incidents to minimise any harm to individuals or the organisation.

This Policy supports the strategic business aims and objectives of Newable by:

- ensuring that it 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 or breaches conform to GDPR requirements and do not conflict with its policies and procedures;
- facilitating the analysis of incident and breach records to determine common threat patterns and existing threat vectors, to raise awareness and implement preventative measures; and,
- ensuring that every member of staff, temporary worker, or consultant understands the importance of reporting and managing information security incidents and breaches to reduce the risk of a future breach and to mitigate the impact of any potential breach.

Purpose

This Policy provides a framework for reporting and managing:

- security incidents affecting Newable's information and information technology;
- losses of information; and,
- near misses and information security concerns.

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

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	Any living individual 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.

Scope

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:

- The loss or theft of data or information.
- Unlawful disclosure or misuse of confidential data or the disclosure of confidential data 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 another significant impact on individuals.
- Inappropriate access controls leading to unauthorised use.
- Any incident that 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 that contain data.
- 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 computer equipment or computer networks.
- Social engineering (or 'blagging') to obtain information by deception.
- Breaches of physical security (e.g., forcing of doors or windows into a secure room, or filing cabinet containing confidential information left unlocked in an accessible area).
- Leaving computer equipment unattended without measures to prevent others from accessing information.

This Policy applies to all users of Newable information and information technology including employees (permanent or temporary), consultants, suppliers, and visitors.

All users must understand and adopt this Policy and are responsible for ensuring the safety and security of the Newable information and information technology that they access or use. This includes data stored electronically and in physical form.

Security of information

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.

Newable 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 include protection measures such as computer passwords, firewalls, and building security, whilst organisational safeguards are aimed at employees, such as ensuring adequate training, policies, and procedures are in place.

Factors that can cause an Incident include:

- Negligence or human error.
- Unauthorised or inappropriate access, including processing confidential personal data without a legal basis.
- Loss or theft of information or equipment containing information.
- Systems or equipment failure.
- Accidents.
- Unforeseen circumstances such as fire, flood, or other environmental factors.
- Inappropriate access, such as viewing information for purposes other than specified or authorised (e.g., an individual browsing a record about an ex-partner to find their current address).
- Unauthorised access, such as using other people’s usernames and passwords.
- Poor physical security.
- Inappropriate access controls allowing unauthorised use.
- Lack of training and awareness.
- Hacking.
- Social engineering (or ‘blagging’) to obtain information by deception.

Procedure for incident handling

All incidents and breaches must be reported as soon as possible to the Data Protection Officer (DPO):

Mashudul Karim
dpo@newable.co.uk
+442079401591

Cyber security incidents

A security event involving information technology, such as a virus found within a malicious email attachment, could spread quickly and cause data loss and/or disruption across the organisation. All users must understand, and be able to identify, unexpected or unusual behaviour on computer equipment, which may not be due to a simple malfunction.

If a user suspects a potential cyber security incident or threat, they should contact the Newable Digital Service Desk as soon as possible on +442079401590 or servicedesk@newable.co.uk. They should also:

- note the symptoms and/or any error messages;
- disconnect affected computer equipment from the network (or internet) or turn them off; and,
- not use any removable storage devices (e.g., USB memory stick) previously used with affected computer equipment.

The DPO and the Newable Digital Service Desk may require further information, which will vary according to the nature and scale of the incident. However, the user must be prepared to supply the following information at a minimum:

- Name and contact details of the person reporting the incident.
- 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 that the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

Other incidents

If the information security event is in relation to paper or hard copy information, such as personal information files stolen from a filing cabinet, this must be reported to Human Resources (HR):

Newable HR Support
hrsupport@newable.co.uk

Collection of evidence

Incidents will often mean that Newable must gather evidence for investigation purposes and adhere to strict rules governing their collection. Newable staff and users must always approach evidence or potential evidence with care.

Breach management plan

There are four essential elements to any breach management plan:

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

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 business such as Digital and HR, and in some cases, contact with external stakeholders and suppliers.

The DPO will consider the following:

- Decide on who should take the lead on investigating the breach (whether the DPO or any other member of staff) and ensure that they have the appropriate resources.
- Establish who they need to make aware of the breach and inform them of what they must 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 they 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 backups 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 that a crime has taken place.
- Where appropriate and deemed material, report any breach of personal data to the ICO.

Assessment of ongoing risks

Before deciding on what steps are necessary following immediate containment, the DPO will 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 has been 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, the actions required to attempt to mitigate those risks.
- What harm can come to those individuals? Are there risks to physical safety or reputation, of monetary loss or a combination of these and other aspects of their life?
- If individuals' bank details have been lost, consider whether to contact the banks themselves for advice on anything they can do to help you prevent fraudulent use.

Breach notification

Mandatory reporting by the DPO to the ICO

Under the GDPR, Newable's DPO must notify the ICO of a breach where it is likely to result in a 'high risk' to the rights and freedoms of individuals.

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 customer names with no further information about the individuals.

This must be assessed on a case-by-case basis. For example, the ICO will need to be notified 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 severity of the personal data breach or 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 DPO should report the incident to the ICO and escalate to other regulators as appropriate. Please refer to *Annex A – Incident Severity Assessment* which will help determine whether an incident is externally reportable.

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 reassessed. Where the numbers of individuals 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.

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 the risk of individuals being identified remains, an incident should be reported.

Timing

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

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

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.

Communicating personal data breaches to individuals affected

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

Informing people and organisations, that a data security breach has occurred, is an essential element in Newable's breach management. Considering the following will assist Newable 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 provided 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 serious consequences, the ICO should be informed.
- Consider how notification can be made appropriate for 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 and notifying a whole two million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work.
- 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 what steps they can take to protect themselves and 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.

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

- Newable has implemented appropriate technical and organisational protection measures in respect of the personal data affected by the breach (such as encryption).

- Newable 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.

The ICO may compel Newable to communicate a personal data breach with affected data subjects or individuals unless one of the three exemptions listed above is satisfied.

Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of Newable's 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 the 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

Incident severity assessment

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

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 (customers) affected.
- The potential for significant distress or damage to the customer.
- The potential for reputational damage to Newable.
- 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).

Loss or theft of computer equipment with encrypted storage or encrypted removal storage devices 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 to decrypt the data has also been lost or compromised);
- the computer equipment was not configured to automatically lock after a brief time without user interaction; or,
- an untested or proprietary encryption algorithm was used.

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

Scale factors

Whilst any personal data breach is a 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.

Sensitivity factors

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 purposes of the incident, sensitivity factors may be:

- low, and thereby reduce the base categorisation; or,
- high, and thereby increase the base categorisation.

Categorising personal data breaches

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

- Level 0 or 1, a confirmed incident but no need to report to ICO and other regulators; or,
- Level 2 or above, a confirmed incident that must be reported to ICO and other regulators.

To determine which category the incident falls under, please refer to *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.

Table 1 – Baseline category based on scale of incident.

BASELINE CATEGORY	DEFINITION
0	Information about fewer 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 2 – Category changes based on sensitivity.

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
	Celebrity involved or other newsworthy aspects or 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 3 – Incident reporting requirements

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)

Notification of data breaches by the DPO to the ICO

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.

Information should include:

- Newable contact details (usually the DPO), stating that Newable 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 that Newable 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.

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

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

Furthermore, Newable 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.

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

Incident management

An individual needs to be assigned to manage the incident (usually the DPO), who will be responsible for communicating and coordinating activities, as well as maintaining an audit trail of events and evidence. An investigation will 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.

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

Personal data breach register

Under the GDPR, both Data Controllers and Data Processors are required to record any personal data breaches and any actions taken. An Internal Breach Register is maintained by the DPO, documenting each incident *“comprising the facts relating to the personal data breach, its effects and the remedial action taken.”*

The ICO has the authority to assess how Newable complies with its data breach notification obligations.

Appendix A

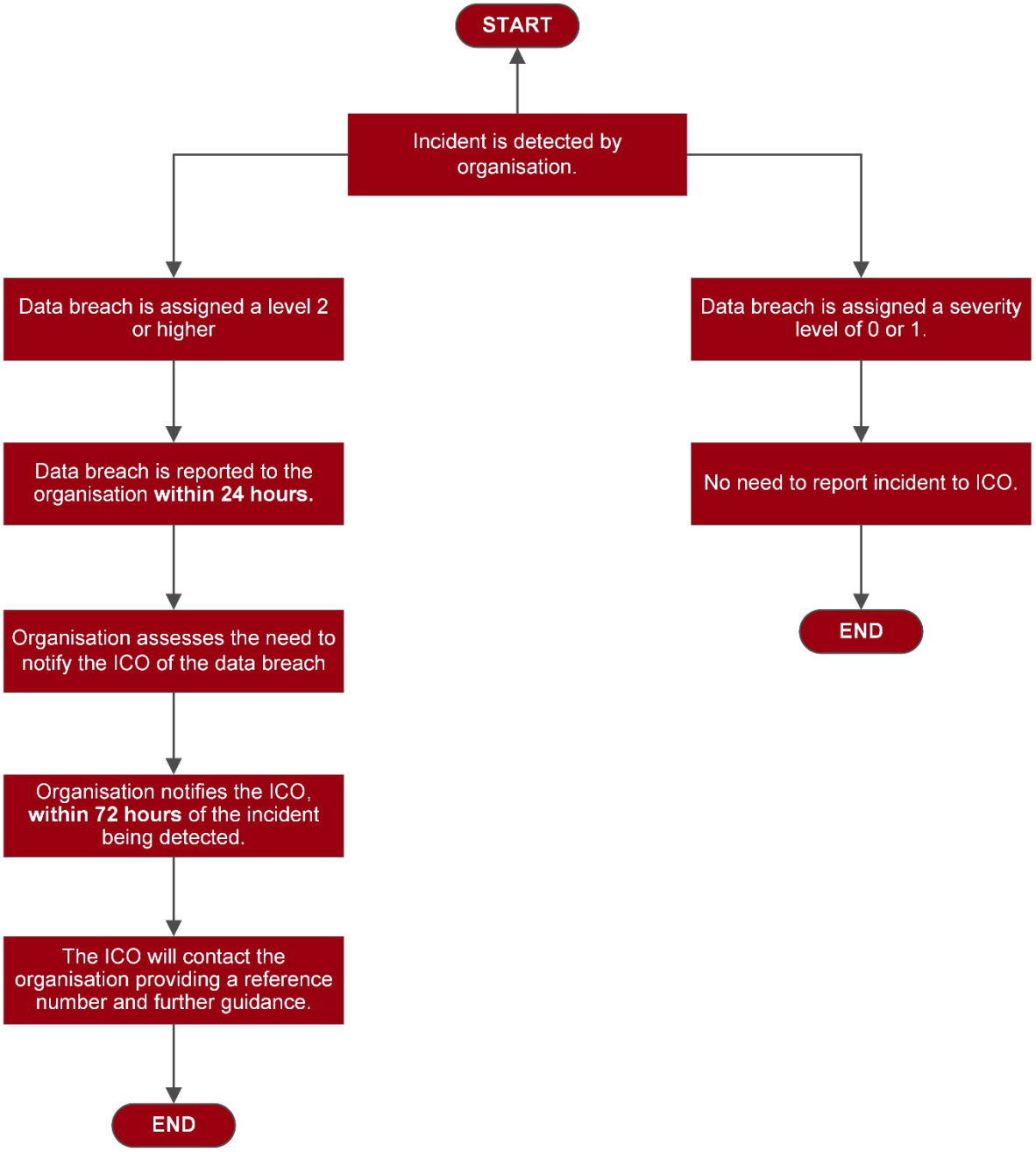
Template to log and report breaches internally

INTERNAL BREACH REPORT FORM		
Date	Time	Location
Name of person reporting incident		
Job title		
Phone number		
Email address		
Description of incident		
Level of incident		
Number of customers 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 Newable DPO Use Only	
Incident reference number	
Received by	
Forwarded for action to	
Remedial action taken	

Appendix B

Breach management flow diagram



Appendix C

ICO breach report template

ICO BREACH REPORT FORM		
Date	Time	Location
Organisation name – Newable		
Name of person reporting incident		
Job title		
Phone number		
Postal address		
Email address		
Description of incident		
Reason for delaying notification, if applicable		

Number of customers affected	
Volume of data affected	
Measures Newable has in place to deal with such incidents	
Potential adverse effects on individuals affected	

Mitigating measures taken	
Have the data been recovered?	
Has Newable reported data breaches to the ICO in the past? If yes, provide details	

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