


| | | | |
|--|--|------------------|---------------------------|
|  RBLI | Royal British Legion Industries GDPR Policy | Author | Scott Gillham |
| | | Effective date | 25 th May 2018 |
| Policy Title | | Reviewed By | Kate Porter |
| Information Security _ Data Breach Incident Response Procedure | | Last Reviewed | June 2021 |
| | | Next review date | July 2021 |

1 Introduction

This document is intended to be used when an incident of some kind has occurred that affects the information security of RBLI, including those potentially affecting personal data for which the organisation is a controller. It is intended to ensure a quick, effective and orderly response to an information security breach.

It is a requirement of the EU General Data Protection Regulation 2018 (GDPR) that incidents affecting personal data that are likely to result in a risk to the rights and freedoms of data subjects must be reported to the data protection supervisory authority without undue delay and where feasible, within 72 hours of becoming aware of it. In the event that the 72-hour target is not met, reasons for the delay must be given.

The procedures set out in this document should be used only as guidance when responding to an incident. The exact nature of an incident and its impact cannot be predicted with any degree of certainty and so it is important that a good degree of common sense and flexibility is used when deciding the actions to take. However, it is intended that the structures set out here will prove useful in allowing the correct actions to be taken more quickly and based on more accurate information.

The objectives of this incident response procedure are to:

- provide a concise overview of how RBLI will respond to an incident
- set out who will respond to an incident and their roles and responsibilities
- describe the facilities that are in place to help with the management of the incident
- define how decisions will be taken with regard to our response to an incident
- explain how communication within the organisation and with external parties will be handled
- provide contact details for key people and external agencies
- define what will happen once the incident is resolved and the responders are stood down

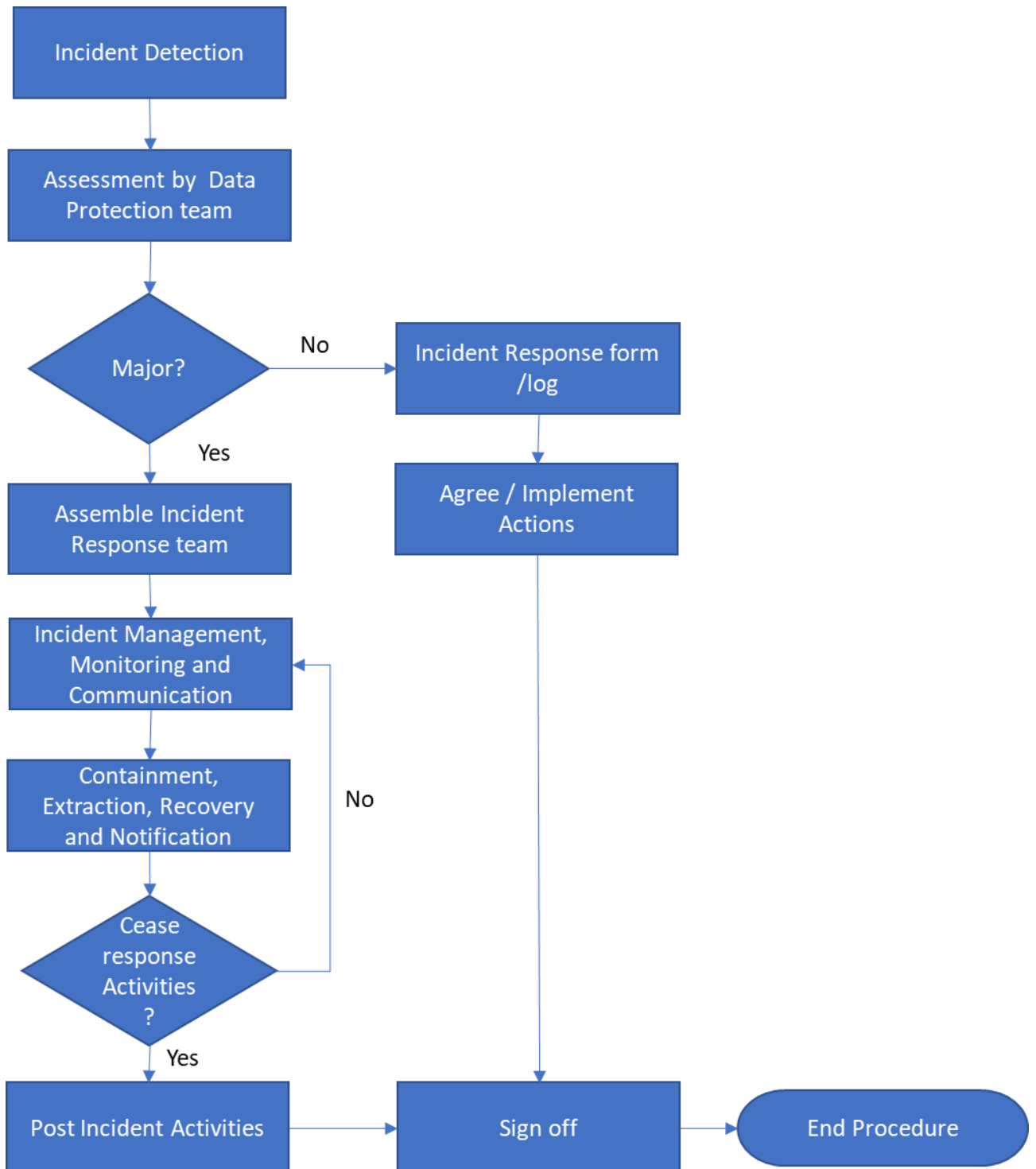
Table of Contents

| | | |
|----------|---|----------|
| 1 | INTRODUCTION..... | 1 |
| 2 | INCIDENT RESPONSE FLOWCHART | 3 |
| 2.1 | INCIDENT DETECTION..... | 4 |
| 2.2 | ASSESSMENT BY DATA PROTECTION TEAM..... | 4 |
| 2.3 | MAJOR INCIDENT? | 4 |
| 2.3.1 | <i>Minor incident</i> | 5 |
| 2.4 | ASSEMBLE INCIDENT RESPONSE TEAM..... | 5 |
| 2.4.1 | <i>Incident Response Team Members</i> | 5 |
| 2.4.2 | <i>Roles and Responsibilities</i> | 6 |
| 2.5 | INCIDENT MANAGEMENT, MONITORING AND COMMUNICATION | 6 |
| 2.5.1 | <i>Communication Procedures</i> | 6 |
| 2.5.2 | <i>Other External Communication</i> | 7 |
| 2.5.3 | <i>Communication with the Media</i> | 7 |
| 2.6 | INCIDENT CONTAINMENT, ERADICATION, RECOVERY AND NOTIFICATION..... | 8 |
| 2.6.1 | <i>Containment</i> | 8 |
| 2.6.2 | <i>Eradication</i> | 9 |
| 2.6.3 | <i>Recovery</i> | 9 |
| 2.6.4 | <i>Notification</i> | 10 |
| 2.7 | POST-INCIDENT ACTIVITY | 13 |

NOTE - All personal information collected as part of the incident response procedure and contained in this document will be used purely for the purposes of information security incident management and is subject to relevant data protection legislation.

2 Incident Response Flowchart

The flow of the incident response procedure is shown in the diagram below.



These steps are explained in more detail in the rest of this procedure.

2.1 Incident Detection

An incident may be initially detected in a wide variety of ways and through a number of different sources, depending on the nature and location of the incident. Some incidents may be self-detected via software tools used within RBLI or by employees noticing unusual activity. Others may be notified by a third party such as a customer, supplier or law enforcement agency who has become aware of a breach perhaps because stolen information has been used in some way for malicious purposes.

It is not unusual for there to be a delay between the origin of the incident and its actual detection; one of the objectives of a proactive approach to information security is to reduce this time period. The most important factor is that the incident response procedure must be started as quickly as possible after detection so that an effective response can be given.

2.2 Assessment by Data Protection Team

Once the incident has been detected, an initial impact assessment must be carried out in order to decide the appropriate response.

This impact assessment should estimate:

- The extent of the impact on IT infrastructure including computers, networks, equipment and accommodation
- The information assets (including personal data) that may be at risk or have been compromised
- The likely duration of the incident i.e. when it may have begun
- The business units affected and the extent of the impact to them
- For breaches affecting personal data, the degree of risk to the rights and freedoms of the data subjects
- Initial indication of the likely cause of the incident

This information should be documented so that a clear time-based understanding of the situation as it emerges is available for current use and later review.

A list of the information assets (including personal data), business activities, products, services, teams and supporting processes that may have been affected by the incident should be created together with an assessment of the extent of the impact.

2.3 Major Incident?

Once notified of an incident the Data Protection Officer must decide whether the scale and actual or potential impact of the incident justifies the activation of the Incident Response Procedure and the convening of an Incident Response Team (IRT).

Guidelines for whether a formal incident response should be initiated for any particular incident of which the Data Protection Officer has been notified are if any of the following apply:

- There is significant actual or potential loss of classified information, including personal data

- There is significant actual or potential disruption to business operations
- There is significant risk to business reputation
- Any other situation which may cause significant impact to the organisation

In the event of disagreement or uncertainty about whether or not to activate an incident response the decision of the Data Protection Officer will be final.

If it is decided not to activate the procedure, then a plan should be created to allow for a lower level response to the incident within normal management channels. This may involve the invocation of relevant procedures at a local level. The Data Protection Officer will be able to offer guidance and advice as to the most appropriate course of action.

If the incident warrants the activation of the IR procedure the Data Protection Officer will assemble the IRT.

If the incident is deemed a major incident the RBLI Serious Incident Reporting Procedure needs to be executed in parallel to this procedure. It may be necessary to include additional organisations into the notification, such as the charities commission or CQC or other steps as determined by the Serious Incident Reporting Procedure.

2.3.1 Minor incident

For a minor incident whilst it is not necessary to assemble the Incident Response Team, the need to understand, record and learn from minor incidents is still required.

As part of the analysis and determining if the incident is major or minor sufficient knowledge should have been obtained to identify what actions could prevent a reoccurrence of the incident. Actions may include user training or update to procedures for example. The incident can be signed off and closed before all actions have been completed, on the basis it remains the responsibility of the Data Protection Team to ensure all actions are completed.

2.4 Assemble Incident Response Team

Once the decision has been made to activate the incident response procedure, the Data Protection Officer will ensure that all role holders or their deputies are contacted, made aware of the nature of the incident and asked to assemble at an appropriate location.

2.4.1 Incident Response Team Members

The Data Protection Officer will ensure that the members of the incident response team are appropriate for the roles needed, taking into account the nature and severity of the incident and any subsequent actions that might need to be taken. Deputies should be identified and notified to ensure continuity throughout the investigation.

2.4.2 Roles and Responsibilities

The key responsibilities and roles within the incident response team are specified in the technology sections of RBLI's Business Continuity Plan. However, these should take account of specific requirements for local knowledge, expertise etc.

Data Protection Officer

- Decides whether or not to initiate a response
- Assembles the incident response team
- Overall management of the incident response team
- Acts as interface with the board and other high-level stakeholders
- Final decision maker in cases of disagreement

Head of Business systems

- Provides input on technology-related issues
- Ensures systems and data are safely secured
- Assists with impact assessment

Head of Estates

- Provided input if the incident relates to buildings

Team Facilitator

- Provides administrative role and communication

2.5 Incident Management, Monitoring and Communication

Once an appropriate response to the incident has been identified, the IRT needs to be able to manage the overall response, monitor the status of the incident and ensure effective communication is taking place at all levels.

Regular IRT meetings must be held at an appropriate frequency decided by the Team Leader. The purpose of these meetings is to ensure that incident management resources are managed effectively and that key decisions are made promptly, based on adequate information. Each meeting will be minuted by the Team Facilitator.

The Incident Liaison will provide updates to the IRT to a frequency decided by the Team Leader. These updates should be co-ordinated with the IRT meetings so that the latest information is available for each meeting.

2.5.1 Communication Procedures

It is vital that effective communications are maintained between all parties involved in the incident response.

The primary means of communication during an incident will initially be face to face and telephone, both landline and mobile. Email should not be used unless permission to do so has been given by the IRT.

The following guidelines should be followed in all communications:

- Be calm and avoid lengthy conversation
- Advise internal team members of the need to refer information requests to the IRT
- If the call is answered by someone other than the contact:
 - Ask if the contact is available elsewhere
 - If they cannot be contacted leave a message to contact you on a given number
 - Do not provide details of the Incident
- Always document call time details, responses and actions

All communications should be clearly and accurately recorded as records may be needed as part of legal action at a later date. The Team Facilitator should be kept informed on all communications

2.5.2 Other External Communication

Depending on the incident there may be a variety of external parties that will be communicated with during the course of the response. It is important that the information released to third parties is managed so that it is timely and accurate.

Calls that are not from agencies directly involved in the incident response (such as the media) should be passed to the member of the IRT responsible for communications.

There may be a number of external parties who, whilst not directly involved in the incident, may be affected by it and need to be alerted to this fact. These may include:

- Customers
- Suppliers
- Shareholders
- Regulatory bodies

The Communications IRT member should make a list of such interested parties and define the message that is to be given to them.

Interested parties who have not been alerted by the IRT may call to obtain information about the incident and its effects. These calls should be recorded in a message log and passed to the Communications member of IRT.

2.5.3 Communication with the Media

In general, the communication strategy with respect to the media will be to issue updates via top management. No members of staff should give an interview with the media unless this is pre-authorised by the IRT.

The preferred interface with the media will be to issue pre-written press releases. In exceptional circumstances a press conference will be held to answer questions about the incident and its effects. It is the responsibility of the Communications IRT member to arrange the venue for these and to liaise with press that may wish to attend.

In drafting a statement for the media the following guidelines should be observed:

- Personal information should be protected at all times
- Stick to the facts and do not speculate about the incident or its cause
- Ensure legal advice is obtained prior to any statements being issued
- Try to pre-empt questions that may reasonably be asked
- Emphasise that a prepared response has been activated and that everything possible is being done

The most appropriate spokesperson will depend upon the scale of the incident and its effect on customers, supplier, the public and other stakeholders.

2.6 Incident Containment, Eradication, Recovery and Notification

2.6.1 Containment

The first step will be to try to stop the incident getting any worse i.e. contain it. In the case of a virus outbreak this may entail disconnecting the affected parts of the network; for a hacking attack it may involve disabling certain profiles or ports on the firewall or perhaps even disconnecting the internal network from the Internet altogether. The specific actions to be performed will depend on the circumstances of the incident.

Note: if it is judged to be likely that digital evidence will need to be collected that will later be used in court, precautions must be taken to ensure that such evidence remains admissible. This means that relevant data must not be changed either deliberately or by accident e.g. by waking up a laptop. It is recommended that specialist advice should be obtained at this point. The Head of Business Systems will identify and facilitate any specialist advice that may be required.

Particularly (but not exclusively) if foul play is suspected in the incident, accurate records must be kept of the actions taken and the evidence gathered in line with digital forensics guidelines. The main principles of these guidelines are as follows:

Principle 1 – Don't change any data. If anything is done that results in the data on the relevant system being altered in any way then this will affect any subsequent court case.

Principle 2 – Only access the original data in exceptional circumstances. A trained specialist will use tools to take a bit copy of any data held in memory, whether it's on a hard disk, flash memory or a SIM card on a phone. All analysis will then take place on the copy and the original should never be touched unless in exceptional circumstances e.g. time is of the essence and gaining information to prevent a further crime is more important than keeping the evidence admissible.

Principle 3 – Always keep an audit trail of what has been done. Forensic tools will do this automatically but this also applies to the first people on the scene. Taking photographs and videos is encouraged as long as nothing is touched to do it.

Principle 4 – The person in charge must ensure that the guidelines are followed.

Prior to the arrival of a specialist basic information should be collected.

This may include:

- Photographs or videos of relevant messages or information
- Manual written records of the chronology of the incident
- Original documents, including records of who found them, where and when
- Details of any witnesses

Once collected, the evidence will be kept in a safe place where it cannot be tampered with and a formal chain of custody established.

The evidence may be required:

- For later analysis as to the cause of the incident
- As forensic evidence for criminal or civil court proceedings
- In support of any compensation negotiations with software or service suppliers

Next, a clear picture of what has happened needs to be established. The extent of the incident and the knock on implications should be ascertained before any kind of containment action can be taken.

Audit logs may be examined to piece together the sequence of events; care should be taken that only secure copies of logs that have not been tampered with are used.

2.6.2 Eradication

Actions to fix the damage caused by the incident, such as deleting malware, must be documented. These actions should be aimed at fixing the current cause and preventing the incident from re-occurring. Any vulnerabilities that have been exploited as part of the incident should be identified.

Depending on the type of incident, eradication may sometimes be unnecessary.

2.6.3 Recovery

During the recovery stage, systems should be restored back to their pre-incident condition, although necessary actions should then be performed to address any vulnerabilities that were exploited as part of the incident. This may involve activities such as installing patches, changing passwords, hardening servers and amending procedures.

2.6.4 Notification

The notification of an information security incident and resulting loss of data is a sensitive issue that must be handled carefully and with full management approval. The IRT will decide, based on legal and other expert advice and as full an understanding of the impact of the incident as possible, what notification is required and the form that it will take.

RBLI will always comply in full with applicable legal and regulatory requirements regarding incident notification and will carefully assess any offerings to be made to parties that may be impacted by the incident, such as credit monitoring services.

Records collected as part of the incident response may be required as part of any resulting investigations by relevant regulatory bodies and RBLI will cooperate in full with such proceedings.

2.6.4.1 Deciding if the breach must be notified

It is not a foregone conclusion that the breach must be notified. This depends upon an assessment of the risk that the breach represents to “the rights and freedoms of natural persons” (GDPR Article 33). This requires that the organisation assess the level of risk before deciding whether or not to notify.

The following sections describe how this decision must be taken and what to do if notification is required.

Factors to be taken into account as part of this risk assessment should include:

- Whether the personal data was encrypted
- If encrypted, the strength of the encryption used
- To what extent the data was pseudonymised (i.e. whether living individuals can reasonably be identified from the data)
- The data items included e.g. name, address, bank details, biometrics
- The volume of data involved
- The number of data subjects affected
- The nature of the breach e.g. theft, accidental destruction
- Any other factors that are deemed to be relevant

Parties involved in this risk assessment may include representatives from the following areas, depending on the nature and circumstances of the personal data breach:

- Senior management
- Relevant areas of the business
- Technology
- Information security
- Legal

- Data protection officer
- Others

The risk assessment method, its reasoning and its conclusions should be fully documented and signed off by top management. The result of the risk assessment should include one of the following conclusions:

1. The personal data breach does not require notification
2. The personal data breach requires notification to the supervisory authority only
3. The personal data breach requires notification both to the supervisory authority and to the affected data subject

These conclusions may be subject to change based on feedback from the supervisory authority and further information that is discovered as part of the ongoing investigation of the breach.

2.6.4.2 What if there is insufficient evidence to complete the assessment?

There may be situations where it is not possible to determine if there has in fact been a data breach. This could happen for example:

- There is a discussion between two people about another individual. The recipient subsequently reports they have been provided personal information they are not authorised to have access to. This is called verbal disclosure. However, as part of the investigation it is not certain what information was shared due to incomplete or conflicting statements. Therefore, the investigation cannot be certain if there was a breach or not
- An individual reports they have been shown personal data they are not authorised to have access to, However, on investigation it is not possible to determine what was shown and if there was a disclosure or not.

In situations where all reasonable steps have been taken to investigate a reported data breach, but the investigation cannot conclude if a breach did in fact occur or not. The investigation shall conclude with the following steps:

- Complete the investigation report to state it has not been possible to establish if a data breach has occurred, and explain why
- Share the outcome with the individual(s) who raised the issue, providing them with an opportunity to respond
- If as part of the investigation there are improvements that could prevent repeated incidents, then these should be actioned.

If the alleged breach could be high risk to the data subject(s), the decision should be to notify both the data subject(s) and the supervisory authority. There is no requirement to report if there is not a data breach but if the risk is significant then

the best approach may be to act as if the breach had occurred even if it could not be proven.

2.6.4.3 Communication to the Data Protection Supervisory Authority

It is a requirement of the EU General Data Protection Regulation 2018 (GDPR) that incidents affecting personal data that are likely to result in a risk to the rights and freedoms of data subjects must be reported to the data protection supervisory authority without undue delay and where feasible, within 72 hours of becoming aware of it. The RBLI *Data Breach Notification Procedure* must be used for this purpose. In the event that the 72-hour target is not met, reasons for the delay must be given.

RBLI Supervisory Authorities:

Health and Care:

If the breach includes data of a resident in Gavin Astor, Queen Elizabeth Court the supervisory authority is the NHS and a report should be made using the NHS Digital Data Security and Protection Incident Reporting tool: <https://digital.nhs.uk/>

For all other data breaches:

All other data breaches need to be reported to the Information Commissioner's Office (ICO): ico.org.uk

The ICO will require the following information to be given as part of the notification:

- a) The nature of the personal data breach, including, where possible:
 - i. Categories and approximate number of data subjects concerned
 - ii. Categories and approximate number of personal data records concerned
- b) Name and contact details of the data protection officer or other contact point where more information may be obtained
- c) A description of the likely consequences of the personal data breach
- d) A description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects
- e) If the notification falls outside of the 72-hour window, the reasons why it was not submitted earlier

Written confirmation should be obtained from the supervisory authority that the personal data breach notification has been received, including the date and time of receipt was received. Where necessary, the GDPR allows the information to be provided in phases without undue further delay.

2.6.4.4 Communication with Personal Data Subjects

Where an incident affects personal data, a decision must be taken by the IRT regarding the extent, timing and content of communication with data subjects. The UK GDPR requires that communication must happen “without undue delay” if the breach is likely to result in “a high risk to the rights and freedoms of natural persons”. The RBLI *Data Breach Notification Procedure* must be used for this purpose.

The risk assessment carried out earlier in this procedure will have determined whether the risk to the rights and freedoms of the data subjects affected is judged to be sufficiently high to justify notification to them.

However, if measures have subsequently been taken to mitigate the high risk to the data subjects, so that it is no longer likely to happen, then communication to the data subjects is not required by the GDPR.

Notification to affected data subjects is also not mandated by the GDPR where it “would involve disproportionate effort” (GDPR Article 34). However, in this case a form of public communication should be used instead. Again, this may change based on feedback from the supervisory authority and further information that is discovered as part of the ongoing investigation of the breach.

How to notify data subjects?

The communication to the affected data subjects “*shall describe in clear and plain language the nature of the personal data breach*” (GDPR Article 34) and must also cover:

- a) Name and contact details of the data protection officer or other contact point where more information may be obtained
- b) A description of the likely consequences of the personal data breach
- c) A description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects

In addition to the points required by the GDPR, it may be appropriate to offer advice to the data subject regarding actions they may be able to take to reduce the risks associated with the personal data breach.

In most cases it will be appropriate to notify affected data subjects via letter or email or both in order to ensure that the message has been received and that they have an opportunity to take any action required.

2.7 Post-Incident Activity

The Team Leader will decide, based on the latest information from the Incident Liaison and other members of the team, the point at which response activities should be ceased and the IRT stood down. Note that the recovery and execution of plans may continue beyond this point but under less formal management control.

This decision will be up to the Team Leader's judgement but should be based upon the following criteria:

- The situation has been fully resolved or is reasonably stable
- The pace of change of the situation has slowed to a point where few decisions are required
- The appropriate response is well underway and recovery plans are progressing to schedule
- The degree of risk to the business has lessened to an acceptable point
- Immediate legal and regulatory responsibilities have been fulfilled

If recovery from the incident is on-going the Team Leader should define the next actions to be taken. These may include:

- Less frequent meetings of the IRT e.g. weekly depending on the circumstances
- Informing all involved parties that the IRT is standing down
- Ensuring that all documentation of the incident is secured
- Requesting that all staff not involved in further work to return to normal duties

All actions taken as part of standing down should be recorded.

After the IRT has been stood down the Team Leader will hold a debrief of all members ideally within 24 hours. The relevant records of the incident will be examined by the IRT to ensure that they reflect actual events and represent a complete and accurate record of the incident.

Any immediate comments or feedback from the team will be recorded.

A more formal post-incident review will be held at a time to be decided by top management according to the magnitude and nature of the incident.