Putting the Community First

BARNET
LONDON BOROUGH

Security and Data Protection Incident Management Policy

London Borough of Barnet

POLICY NAME	Security and Data Protection Incident Management Policy		
Document Description	Policy which sets out the council's approach to managing information security incidents, physical security incidents and data protection incidents and which gives guidance for staff on how to report these incidents and procedures to follow.		
Document Author 1) Team and 2) Officer and contact details	1) Information Management Team 2) Sarah Laws x 2587 sarah.laws@barnet.gov.uk		
Status (Live/ Draft/ Withdrawn)	Live	**Version**	04.00
Last Review Date	February 2016	**Next Review Due Date**	March 2017
Approval Chain:	Security Forum	**Date Approved**	08/03/2016

Version Control

Version number	Date	Author	Reason for New Version
V0	28 Sept 2012	D. Hunt	Draft
V1	1 Oct 2012	D Hunt	First Issue
V2	29/10/12	L Wicks	Merging with DP Incident Reporting Policy
V2.1	31/12/13	L Martin	Annual Review
V2.2	13/06/14	S Laws	Updates to PSN and addition of premises security section, other minor amendments
V2.3	09/12/2014	S Laws	Further substantial rewrites following security forum
V3.0	19/12/2014	Sarah Laws	Final amendments, approved version from Security Forum
V3.01	13/5/2015	Sarah Laws	Amendment to title of IT Security Manager
V04.00	27/01/2016	Sarah Laws	Annual Review

Contents

1. Introduction

1.1. Purpose and Scope

The purpose of this document is to describe the procedures for identifying, reporting, responding to and learning from security incidents, threats or vulnerabilities whether actual, suspected or perceived. This policy and its procedures are applicable to all aspects of the council's operations whether electronic, non-electronic, premises or infrastructure and personnel (apart from health and safety threats to people – see below).

All systems and activities will be subject to formal incident recording and escalation procedures. There are separate procedures for IS Security Incidents, Data Protection Incidents and Premises Security Incidents.

NB Threats and safety incidents regarding personnel are out of scope of this policy. The Health and Safety Reporting Policy or the Potentially Violent Persons Policy (currently draft) should be used instead where appropriate and advice sought if necessary from the Head of Health, Safety and Welfare.

Incident recording will be used to log all untoward events. This mechanism must include what happened, what was done and the resolution.

Several organisations and items are referred to in this policy.

Public Services Network (PSN). The council has a connection to the Public Services Network which provides a secure network for organisations across central and local government and the wider public sector. Connection to this network is essential for the effective running of many council services and our continuing access is dependent on us meeting a set of security and other standards.

The PCI Security Standards Council. Any organisation like the council that takes payments by credit or debit card has to adhere to a set of standards published by the PCI Security Standards Council. The PCI Council is an open global forum for the ongoing development and implementation of security standards for payment data protection. More detailed information can be found here

Data Protection Act 1998 (DPA). The DPA is an Act which regulates how the council uses, stores, collects, destroys etc ("processes") information which relates to identifiable individuals (personal information). More information on how the council complies with the DPA and the council's DPA policies is available on the Information Management page of the intranet.

Information Commissioner's Office (ICO). The ICO is the regulator for organisations' compliance with the Data Protection Act amongst other areas of responsibility. They have the powers to investigate data incidents reported to them and in some circumstances can issue fines. Their website is www.ico.org.uk

Communications Electronics Security Group (CESG). The UK government's National Technical Authority for Information Assurance is known as CESG. It advises organisations on how to protect their information and information systems against today's threats.

Security Forum

The purpose of the council's Security Forum is:

- To monitor and mitigate the council's exposure to security (information and physical) risk.
- To oversee compliance with security policies and procedures, and to ensure that these remain appropriate and fit for purpose.
- To monitor breaches in security and to recommend follow-up action.
- To provide a central management point for matters relating to security.

All internal delivery units are represented on this group, along with the Commissioning Group, CSG, Re and The Barnet Group. Representation is regularly reviewed and other external delivery units are likely to be added as needed when they come into being.

Structure of this policy.

This document is split into two parts:

1. Policy: which sets out the council's policy and approach to this area and

2. Procedure: which sets out the practical steps to be taken when incidents occur.

2. PART 1 - POLICY

2.1. Policy Objective

The objective of Security and Data Protection Incident Reporting and Management Policy is to detect, investigate and resolve any actual, suspected or potential breaches of security, and to take action that will avoid, or reduce the impact or probability of a further similar reoccurrence.

A security incident is an event which causes or has the potential to cause:

- Reduced or weakened system access or integrity
- Loss of system or information availability
- Loss of or inappropriate disclosure of personal data or business sensitive information, whether electronic or on paper, or any other form including verbal conversation
- Corruption of information

- Disruption of activity
- Financial loss including unauthorised disclosure of payment card information
- Legal action
- Unauthorised access to applications or information
- Unauthorised access to premises
- Suspicious package unattended in building/ bomb threat etc

Specific incidents concerning breaches or suspected breaches of the Data Protection Act (DPA) (affecting personal data) are addressed in Section 3 of this policy and must be handled by the council's Data Protection Officer and in line with the DPA requirements.

The Data Protection Officer works in the Information Management Team (IMT) and Information Management Officer colleagues in IMT routinely undertake work on their behalf.

Specific incidents concerning building and premises threats and safety are addressed in section 5.4 of this policy.

Examples of incidents could include activity such as:

Activity	**Type of Incident**
Attempts (either failed or successful) to gain unauthorised access to a system or theft of its data	IS security incident, and where theft or inappropriate disclosure concerning personal information, a data protection incident as well
Unwanted disruption or denial of service	IS security incident
The unauthorised use of a system for the processing or storage of data	IS security incident, and where usage includes personal information, a data protection incident as well
Inappropriate access controls allowing unauthorised use	IS security incident, and where usage includes personal information, a data protection incident as well

Human error such as choosing the wrong recipient name from a drop down address book menu when selecting an email address	Data protection incident
Equipment failure or unforeseen circumstances such as fire or flood	IS security incident and where personal data is destroyed or made permanently unavailable a data protection incident as well
Inappropriate alteration or deletion of information outside of usual process or retention timescales	Data protection incident, and if if a result of a system or process failure an or IS security incident as well
Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent	IS security incident and where the changes trigger an automated action which affects the data data protection incident as well.
Loss of removable media (USB Stick, Disc etc) and portable equipment (Laptops/Tablet PCs)	IS security incident, and where personal information also lost or media is unencrypted a data protection incident as well.
Tampering/attempting to tamper with CCTV cameras or the leaking of unauthorised film footage taken from CCTV equipment	IS security incident and a data protection incident
Loss of paper files containing personal or confidential data	Data protection incident
“Blagging” or social engineering where information is obtained by deceiving the organisation who holds it	Data protection incident
Emails (unless from IS) warning of viruses, unsolicited emails containing attachments that have	IS security incident

.exe files attached	
Letters, documents, emails etc addressed to one person being sent to another person as well or instead of the correct person	Data protection incident
Unauthorised person(s) gaining access into council premises	Premises security incident and possible data protection incident if access suggests personal data has been compromised

2.2. Scope and Responsibilities

This policy applies to partners/contractors such as Re, CSG, NSL and all permanent, contract and temporary employees, and all third parties (for example employees of Re, CSG) who have access to LBB premises, systems or information. We refer to all these as “Everyone” in this policy. Everyone must familiairse themselves fully with this policy and ensure that its terms are complied with.

Everyone is personally responsible for ensuring that security breaches do not occur as a result of their actions. Everyone must be aware of their responsibility to report any potential, suspected or actual incident such as those described in 2.1 above. Reporting is covered in Part 2 below.

Security breaches (or near-misses) caused knowingly and deliberately, by reckless behaviour, or non-compliance with Information Management policies including the non-reporting of an incident, may result in action being taken in relation to the conduct, capability or performance of the person concerned. This also includes accessing data without justifiable cause or for personal gain or interest.

Action may include formal action in line with the council’s policies, codes of conduct and employee handbook. A severe breach, resulting in loss, maladministration or putting vulnerable clients at risk could constitute gross misconduct. It is the responsibility of each individual to understand where to find the latest policies and procedures for how the council uses, processes and protects personal and sensitive data.

The responsibility for investigating incidents lies with Facilities Management IS, Information Management Team (IMT) as necessary depending on the type of incident.

Responsibilities for reporting and dealing with incidents

The duty to **immediately** report the incident is the responsibility of the person who:

- is using the affected equipment

- discovers the Data Protection incident
- discovers the security incident

Reporting **must not be delayed** due to e.g. annual leave/ absence of managers/ workloads.

Reporting must be treated as a service priority.

Reporting is dealt with in Part 2 in sections 4 onwards– Procedure for Reporting Incidents.

3. Responsibility for Dealing with Incidents

Everyone has a duty to assist and cooperate with the investigation of Security and Data Protection Incidents. Prompt and willing cooperation and assistance with investigations is expected of everyone.

3.1. Senior Managers

- Cooperate with any investigation into the incident and assist where required in the coordination and collection of information
- Ensure that any actions and agreed remediation arising out of an incident are implemented

3.2. IS Team

- Complete remaining sections of the Security Incident Report Form and allocate reference
- Advise the IS Service Delivery Manager and the IT Security Manager immediately
- Liaise with the Information Management Team as appropriate
- Ensure the incident is recorded correctly in the help desk system. If the incident is of a very high or high severity use the Capita Major Incident Management (MIM) process to manage the process and record actions throughout the period until resolution
- Maintain library of completed records
- Ensure the requirements of the Capita incident reporting policies are met

3.3. Data Protection Officer

- Fully investigate incident and undertake initial risk assessment to determine seriousness of incident
- Delegate investigation and risk assessment in whole or part to suitably qualified colleague as appropriate
- Escalate as appropriate depending of severity of the incident
- Undertake or request others to undertake appropriate mitigation of an incident
- Make recommendations and assign actions following findings of investigation to mitigate against further incidents
- Liaise with IS as appropriate

- Decide on reporting to third parties or governing bodies
- The Data Protection Officer (or a colleague nominated by them) will also liaise with colleagues and external bodies or other third parties as required on safeguarding issues where there are urgent safeguarding concerns

3.4. IT Security Manager

- Allocate severity and priority to the incident and agree resolution action plan
- Work with the Data Protection Officer in event of a data protection incident (an incident which involves personal data)
- Manage and monitor resolution of all IS related incidents
- Advise and involve other parties as appropriate, including escalation within the council. Other parties may include emergency response teams
- Review resolved incident and manage activities in conjunction with the Capita Major Incident management Policy, the Service Delivery Manager (SDM) and Capita senior management as required to avoid or reduce the probability of reoccurrence and the potential impact of any future incidents
- Approve closure of resolved incidents
- Provide reports of incidents as required to the Security Forum
- Advise the Information Security for London (ISfL) (a forum for the Information Security officers of the London boroughs and associated public sector organisations) as and when required
- Advise the PSN Network bridge if the incident is notifiable under PSN contracts, or acquiring banks if required by the Payment Card Industry regulations

3.5. Risk Assessment and Incident Containment and Recovery

3.5.1. Incident Management

The Data Protection Officer will work closely alongside the IT Security Manager and affected delivery units in managing and co-ordinating the investigation. Key decisions to be made will be:

- to determine a lead and assign further roles as appropriate
- to establish whether there is anything we can do to recover any losses or to limit the damage
- identifying immediate risks that need to be mitigated
- identifying who to inform - Corporate Anti-Fraud Team, police etc
- identifying other third parties who could assist in limiting the effects of the loss

The incident will be logged on the council's incident register and a full audit trail of information gathered during the containment, recovery and assessment process will be retained in line with the council's retention policy.

An incident report will be produced together with a risk assessment for the incident and any associated risks identified.

Depending on the nature or seriousness of the incident and the risks identified it may be appropriate to produce an action plan with assigned tasks and target times. The delivery unit Information Management Governance Group (IMGG) will monitor the agreed actions and should be regularly advised of progress. Completed actions will be marked on the incident register. See section 7 below for more details.

3.5.2. Risk assessment

An integral part of the process will be identifying risks, whether these are IS, data protection, wider information management, premises security or other risks. The process will also include quantifying and assessing the risks and identifying mitigating actions required to eradicate the risks or to reduce them to tolerable levels. Risk assessments may be needed at different stages of the investigation process.

Risk management is about the cultures, processes and structure inherent within the council that are directed towards the effective management of potential opportunities and threats. The council's Risk Management Framework (available on the link above) is to proactively identify, understand and manage both risks inherent in the delivery of council services and associated with the council's plans and strategies, so as to encourage responsible, informed risk taking. The framework includes a risk matrix, based upon current best practice in the public sector. It is based upon a 5 by 5 matrix of impact and probability. The Risk Management Framework should be read and its approach followed by all staff investigating incidents.

The Security Forum Risk Management Approach Document sets out how the Forum manages risk. It states that the Security Forum will take a risk-based approach to decision making. It does this by:

- when a risk is identified, ensure appropriate action is taken to assess the risk, using the risk assessment form
- once a risk is agreed, ensure it is assigned an appropriate owner and managed in the council's risk management system, JCAD
- identify potential dependencies between risks
- advise on risk appetite for security risks, deciding what is an acceptable amount of risk to accept and escalate
- consider risk in aggregate or the net effect of multiple risks coming to fruition.

The Risk Management and Incident Reporting process has been summarised in a visual flow chart format which is contained in Appendix G.

4. PART 2 PROCEDURE FOR REPORTING INCIDENTS

4.1. Reporting Incidents – Instructions for Everyone

Incident Type	Report to	Contact Details	Any other actions required
Data Protection incident or suspected incident	Information Management Team	ext 2029 data.protection@barnet.gov.uk	Complete an Incident Report Form (located as Appendix A of this policy). Provide as much information as possible. Where documents or removable media are involved store these in a locked cabinet until they are handed over to IMT
Suspected infection of computer equipment by a virus or malicious code	IT service desk	ext 3333 ITServicedesk@Barnet.gov.uk	Complete an Incident Report Form (located as Appendix A of this policy) and provide further information or evidence as and when requested. IS will advise what to do on a case by case basis.
Any other IS security issue	IS service desk	ext 3333 ITServicedesk@Barnet.gov.uk	Complete an Incident Report Form (located as Appendix A of this policy) and provide further information or evidence as and when requested. IS Security will advise what to do on a case by case basis.
Physical Security eg intruder or door access controls broken	Facilities Manager	ext 7269 sean.patten@barnet.gov.uk	The incident should be described as fully as possible. There is no standard form to complete.

4.2. Initial Reporting - Delivery Unit's Risk Assessment

The affected delivery unit will be required to complete an initial risk assessment which must as a minimum contain:

- type of breach or incident
- the type of personal data involved and the sensitivity of it
- the volume of personal data involved
- number of data subjects affected
- the likely level / type of harm that could be caused to data subjects
- the potential harm to the council or third parties (reputational, media interest etc)
- security precautions already in place
- details of any action already taken following the incident
- A timeline of events to date

5. Reporting a Data Protection incident

Any incident either actual or suspected which involves the loss, unlawful disclosure or suspected misuse of personal data **must be immediately reported** to the council's Information Management Team who will ensure that it is handled in accordance with the requirements of the Information Commissioner's Office (ICO). This may also involve reporting via the PSN and the PCI.

Examples of what may need to be reported are given in section 2.1 above. It is important that both incidents and suspected incidents are reported. The council investigates 'near misses' as well as incidents. (Near misses are incidents which would have occurred were they not caught in time.).

Examples of incidents and near misses are:

- a lost case file
- a report being sent to the wrong email or postal address
- a wrong person (council employee or other) being sent an email containing personal information
- a check on outgoing post finding wrongly enveloped letters
- a case file being found left in a meeting room

Timeliness of reporting is key to ensure measures are put in place to contain the damage and begin the recovery process.

Incidents can either be logged by email at **data.protection@barnet.gov.uk** or by calling ext 2029. You will be asked to complete an Incident Reporting Form, located at Appendix A.

It is important that you provide as much information as possible, to allow a clear and quick understanding of the potential risk involved.

5.1. Notification

It is important to consider the element of notification when dealing with a data / security breach. It is not just a case of determining whether or not to notify to the Information Commissioner's Office (ICO), PSN, or PCI but also other considerations such as notifying the data subjects, other regulatory bodies, and management teams and other third parties who may be liable and are able to limit the possible damage resulting from the loss.

Notification of third parties (including the data subjects concerned) where there are DPA issues should only be carried out with prior approval of the Data Protection Officer.

Things to consider when deciding whether to notify:

- To assist the data subject(s) involved (for example to allow them to take appropriate data security measures or to be extra vigilant)
- To comply with our legal or contractual requirements
- To assist in damage limitation
- To enable third parties to take appropriate mitigating actions

This is not a definitive list, but an indication of areas which may be useful to bear in mind.

Safeguarding Issues: There may be occasions where information or individuals concerned in an incident have safeguarding implications. Where this is the case safeguarding takes precedence. However, unless the matter is a matter of immediate life or death, the notifying of individuals for safeguarding reasons should be discussed with the DP Officer before notification takes place.

Once you have decided who you need to notify you should also consider how this is going to be done and what method of communication you are going to use. A record must be kept of all notifications made.

If the data loss affects a number of individuals which may increase enquiries then perhaps a dedicated helpline and resources is deemed appropriate to deal with this.

You may also feel it appropriate that the media ought to be notified. In this case please contact the Communications Team with full details of the incident, including the measures put in place and actions taken to deal with the incident.

All press releases in relation to data loss will be coordinated through the Corporate Communications team but must be undertaken with the assistance of the Data Protection Officer.

5.2. Notification to the Information Commissioner's Office

The Information Commissioner's Office (ICO) is the regulatory body which oversees compliance with the Data Protection Act.

Although there is no legal obligation on data controllers to report breaches of security, which result in the loss or disclosure of personal data, the Information Commissioner does believe serious breaches should be brought to the attention of his Office.

All notifications to the ICO must be agreed and actioned by the Data Protection Officer in liaison with the Senior Information Risk Owner.

In some circumstances it may be appropriate to report an incident even if the volume of data involved is relatively low, specifically where the risk is particularly high perhaps in regards to the sensitivity of the data or the amount lost in regards to an individual.

ICO guidance should be referred to when assessing the seriousness of a breach and the decision to notify.

5.3. Reporting a Physical or Premises Security Incident

The security of premises occupied by the council is essential to safeguard the council's information and its equipment and also to ensure the safety of everyone present on the premises. Part of the council's PSN requirements are that premises security is ensured and breaches are dealt with appropriately.

Premises security requirements are to be covered in the proposed Premises Security Policy.

5.4. Premises Incidents

It is not possible to give a definitive list of what may be a premises security incident. They may range from minor – a visitor is not wearing a visitor badge, to more serious – a suspect package left unattended for a period of time. They will include all incidences where unauthorised access is gained to council premises.

When dealing with premises security incidences using common sense is essential.

The following are indicative guidelines:

- If you see a person who is not wearing ID or a visitor's badge who you do not know, you should ask them to show appropriate identification. If they cannot provide this you should ask them why they are in the building. If you are not satisfied with the response you should ask the person to accompany you to reception. They can then wait until they are collected by an appropriate person and can be given the necessary badge or escorted from the premises.

- N.B. If you do not feel able to challenge someone in this way or if the person does not respond, is unwilling to accompany you, or is aggressive, then you must immediately report this to reception, security or the custodian on ext 2222. A description of the person and their last known location should be provided.
- If a package is seen unattended it should not immediately be assumed to be suspect. Do not touch the package but ask around the immediate vicinity to see if it belongs to anyone or if anyone knows whose it may be. If after a reasonable search an owner cannot be located contact the custodians on ext 2222 to report the matter.

5.5. Loss/ Theft/ Damage

In the unfortunate event of loss or theft of items the following processes should be followed.

•Personal Property

Please report losses, theft or damage to personal property on council premises or during council duties to all of the following:

- your line manager
- the police
- and where appropriate your insurance company for claim purposes.

The council accepts no liability for any theft/damage to personal property. There is guidance on keeping your personal property secure in the Information Security Policy.

•Council Property

If you lose any council property whether in council offices, at another location or whilst travelling, this must be reported. All thefts of council property need to be reported wherever the theft has occurred. Please report the loss or theft of council property to **all** of the following:

- your line manager
- the police (Obtain a crime reference number from the police, as this will be required for claim purposes)
- the Information Management Team on ext: 2029

- Insurance on ext: 7195 and
- Service Desk on 020-8359-3333 during office hours or 020-8202-4488 outside office hours.

Damage to council property should be reported as above but the police do not need to be informed unless it has been caused maliciously.

5.6. Investigation

The Facilities Management Team will investigate premises security issues reported to them as needed on a case by case basis. They will make recommendations for mitigating actions and policy amendments as required.

Facilities management will liaise with IS Security and the Information Management Team as necessary when resolving a premises incident.

5.7. Reporting

Following an incident a report detailing all the relevant information should be sent to facilities management who will then investigate and pass to the appropriate delivery units.

6. IS Management of Incidents

6.1. Applicability of this Section

This section applies to the management of IS security incidents which are not data protection or premises security incidents.

6.2. Procedure

This section describes the procedure to be followed, but as every incident is different, common sense should be used to ensure that incidents are resolved with appropriate priority according to their severity.

Prompt action may be necessary to reduce the potential impact of an incident, so there may be times when an incident is resolved before it is recorded. If this occurs, an incident report form in Appendix A should be completed as soon as possible after the event.

It is important that every incident, however minor, is recorded and follows this procedure to ensure that the probability of reoccurrence is reduced, and the impact of future incidents is minimised. (See Appendix C for further information).

6.3. Recording

Every reported incident will be recorded in the security incident queue in the helpdesk system and recorded in the log kept by the IT Security manager

The help desk will allocate a Reference Number and record the details on the incident report progress record.

IS will keep the records up to date as resolution progresses and a central record is kept by the IT Security Manager. All security incidents are reported routinely to the Security Forum. See Appendix G for the flow chart for reporting.

Potential incidents or identified weaknesses will be recorded on an Incident Record form and this procedure will be followed, but will not go through the Resolution, escalation or reporting stages.

6.4. Prioritisation

Once the incident has been recorded, it will be prioritised according to severity. This will be based upon the actual or potential impact of the incident upon the council's systems and information.

The categories are:

- Critical (C)
- High (H)
- Medium (M)
- Low (L)

These are not to be confused with the PSN classifications (see 6.8 below).

Security incidents are allocated an incident level based on the impact they are likely to have. These are: Emergency, Major, Warning and Information.

6.5. Resolution

The incident will be allocated to an individual or team, and a resolution action plan will be produced with target resolution times. The resources used to resolve the incident will depend upon the identified severity level, for example in the case of a low severity "no action" may be an acceptable option if the resources required outweigh the impact.

The IT Security Manager will monitor the resolution, and reporting where it is required or necessary.

6.6. Escalation

Every IT security incident that may have an impact on the council or its customers will be reported immediately to the IT Security Manager in order to ensure that appropriate priority and resources are allocated to resolving the incident. It may be appropriate that other officers / organisations have to be contacted

- The council's Security Forum

- If appropriate the ICO

- If appropriate inform the PSN, PCI and CESG in accordance with the requirements of the guidance contained in the Incident and Problem Management for the Public Services Network Programme, (latest issue).or the latest issue of the PCI guidance. Contacts with the PSN and the definition of authority are recorded in the LB Barnet London PSN Master Contact List. See the section on PSN below

- Information Security for London (ISfL) is a forum for the Information Security officers of the London boroughs and associated public sector organisations. Facilitated by London Councils Capital Ambition Programme it allows the boroughs to get together on a regular basis to share good practice, exchange views and address security issues that could potentially be affecting everyone.

- If appropriate GovCertUK (see Appendix B) a body that assists government departments and organisations in the recovery from a computer security incident using the appropriate reporting template (see Appendix D) and emailed to incident@govcert.gov.uk . Further details can be found at http://www.govcertuk.gov.uk/reporting-an-incident.shtml

6.7. Reporting to Security Forum

On resolution of the incident, the actions taken will be recorded on the Security Incident Report Form, which will be forwarded to the IS Service Delivery Manager and the IT Security Manager. They will report to the Security Forum as required.

6.8. PSN

Incidents that affect the PSN are categorised as follows:

Incident Any unplanned interruption to a service or a reduction in the quality of a service

Major Incident An incident that results in significant disruption to the public sector organisations

Security Incident Any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or loss or denial of availability

Problem The root cause or potential cause of one or more incidents. It is mandatory that the PSN security manager is informed of any incident classed as Major or Emergency. The responsibility for doing this lies with the IT Security Manager.

Other PSN obligations include:

- The council must undertake an initial diagnosis of incidents to determine which service is the cause/most likely cause of the Incident

- The council must raise incidents with service providers with whom the council has a supply agreement for the affected service

- There is an expectation that the council will inform the PSN if there is a problem that has a broad impact on the PSN

Therefore it is essential that all security incidents are reported promptly.

The appropriate PSN reporting form is in Appendix D

7. Evaluation and response of incidents

This section applies to all incidents covered in this policy.

Following the investigation of an incident, regardless of the circumstance, it is important to learn from mistakes and improve security. These learning points may be case/incident specific or they may apply to the council as a whole. The investigating officer will bring the learning points and any actions required in connection with the incident to the attention of the relevant delivery unit. Where significant issues have been noted actions will be escalated within the council as needed.

All incidents must be reviewed by the IT Security Manager or their nominated colleague to ascertain whether there is a risk of reoccurrence. If there is no such risk the IS and premises (where applicable) incident records will be closed. All potential vulnerabilities will be assessed, recommendations made to mitigate the risk and appropriate action taken to ensure that the risk is kept to an acceptable level. New or revised controls should be implemented as is necessary.

If appropriate, service risk registers must be updated to reflect the ongoing risk

For data protection incidents, where actions have been noted as required, which are significant or substantial in content or volume, these actions will be recorded in the data incident report. A risk assessment will be completed together with remedial actions required to remove the risks or to reduce them to a tolerable level. These will be reported to the relevant Information Management Governance Group (IMGG). The monitoring of progress of the actions will be undertaken by the relevant IMGG and logged on the incident register by the Information Management Team.

PCI incidents and breaches must initially reported to the Acquirer, (Barclaycard or Worldpay). The current contacts for these organisations are shown in Appendix F

In case of a PCI breach the PCI council guidance should be followed regarding preservation of evidence etc.

8. Closure of incidents

Each IS security incident will remain open until it has been satisfactorily resolved, appropriate documentation and/or report completed, and actions taken to avoid reoccurrence, or to ensure the impact of reoccurrence is at an acceptable level and that risks are minimized.

The closure of IS incidents will be jointly approved by the IS Service Delivery Manager, relevant Director or Data Protection Officer as is appropriate.

Data protection incidents will be closed in conjunction with the Information Management Team when immediate mitigating actions have been completed. Further work by IMT or delivery units may be required on an incident following the incident closure.

Premises security incidents will be closed by the Operations Manager once mitigating actions have been completed.

9. Review

This policy will be reviewed annually unless law, policy or other developments require an earlier change.

10. Contact Information/Further Guidance

Further advice and guidance on data protection is available from the Data Protection Officer.

Tel No:	020-8359-2029
Email:	data.protection@barnet.gov.uk

Or on IS the Information System Team: -

Tel No:	020-8359-3333
Email:	itservicedesk@barnet.gov.uk or ICT.Security@barnet.gov.uk

Or on building / premises security from the Facilities Management

Tel No:	(020) 8359 7269
Email:	sean.patten@barnet.gov.uk

11. Appendix A - Security & Data Protection Incident Report Form

Ref No: -	

FOLLOWING SECTIONS TO BE COMPLETED BY REPORTING OFFICER			
Name of Reporting Officer:			
Contact Telephone Number:			
Name of individual(s) involved in incident if different from above:			
Date incident occurred: -			
Type of incident: -			
Systems or information affected: -			
Delivery unit(s) affected: -			
Allocated to: - ***(for use by IS)***		Date: -	
Description of incident and impact: -			
 Severity (if known):			

Full detail the information affected e.g. lost / stolen / mis-used etc:

(Please include all paper records, electronic devices, and RSA fob and be as detailed as possible)

Details of any actions you have taken to date:

FOLLOWING SECTIONS TO BE COMPLETED BY IS WHERE RELEVANT

Summary of Findings and action plan: -

Sent to: - (Name of Manager)

Action Plan Sent: - *(Date)*

Summary of Action Taken including escalation: -

Action taken by: -

Action taken: - *(Date)*

Review and actions taken to avoid reoccurrence (include change control refs, business continuity plan and risk assessment): -

Action taken by: -

Action taken: - *(Date)*

Date Closed: -	**/**/****		
IS Manager:		**Head of IS**	

12. Appendix B – FOR IS STAFF USE ONLY- Guidance for Reporting Electronic Attack Incidents

Introduction

From the first of February 2007 CESG, as the National Technical authority for Information Assurance (IA), has assumed the lead responsibility within UK Government for providing IA advice to public sector organisations. This role includes providing an emergency response capability to public sector organisations that may require technical support and advice during periods of electronic attack or other network security incidents

To facilitate the provision of incident response operations to Government, CESG has formed a dedicated team to operate a CERT (Computer Emergency Response Team) function, with this team being identified to the Government community as GovCertUK.

The CESG GovCertUK Incident Response team provides a 24/7 (24 hours 7 days a week) operation, and can be contacted on the following:

Telephone:	01242 709311
Fax:	01242 709113

General Enquiries: enquiries@govcertuk.gov.uk or govcertuk@cesg.gsi.gov.uk

Incidents & Alerts: incidents@govcertuk.gov.uk or govcertuk@cesg.gsi.gov.uk

During Office hours 0830hrs – 1700hrs all correspondence will be monitored by the GovCertUK response team. Outside office hours, weekends, and public holidays, all correspondence will be monitored by a duty officer, supported by on-call GovCertUK response personnel

One of CESG's roles is to minimize the risk and effects of electronic attack to the government community. As CESG's Computer Emergency Response Team, GovCertUK assists government departments and organisations in the recovery from a computer security incident. They gather data from all available sources to monitor the general threat level and focus. For these reasons the early reporting of incidents and attempted attacks is highly recommended

To assist in the identification and categorisation of an event please read GovCertUK's Incident Response Guidelines (pdf) for further information and guidance.

Reporting Process

Incidents should be reported on telephone number 01242 709311 for an initial response, which should be followed up with an email to incidents@govcertuk.gov.uk using the incident template (doc).

During office hours (0830 -1700) all correspondence is monitored by the GovCertUK response team. Outside office hours, at weekends and on public holidays all correspondence will be monitored by a non-specialist duty officer, supported by on-call GovCertUK response personnel. When speaking to the duty officer, please be clear that the call is for GovCertUK.

Where possible as much supporting information as possible should be supplied, such as log files, internal/external IP addresses, affected operating systems, patch levels and policy etc.

How to submit malware samples to GovCertUK

All samples should be sent by carefully following the procedures below:

- All samples should be renamed to <origninalfilename>.<orginalfileextension>.txt
- All samples should then be zipped and password protected with the password 'infected'
- Optionally (but recommended), PGP encrypt the message (and attachments) with the GovCertUK Public Key, available here
- Use the following subject line: 'MALWARE SAMPLE'
- Send the message to samples@govcertuk.gov.uk

NB: To submit malware samples that are classified, are from classified systems or contain sensitive information please contact GovCERTUK for instructions.

GovCertUK
A2f
CESG
P.O. Box 144, Cheltenham
Gloucestershire
GL51 0EX
UK

13. Appendix C - Management and recovery plan of a reported IS incident

Incident

Classification - *What type of incident has occurred?*

- Loss of confidentiality of information
- Compromise of integrity of information
- Denial of Service
- Misuse of Service
- Damage to Systems

Priority and Urgency - *Identify the response level of effort for a given type of incident.*

- Threats to the physical safety of human beings
- Root or system level attacks to any host or system
- Compromise of restricted confidential service accounts or software areas
- Denial of service attacks to infrastructure, confidential service accounts or software areas
- Any of the above at other sites which originate from the organisation's systems
- Large scale attacks of any kind (worms, sniffing attacks, etc)
- Threats, harassment, or criminal offences involving individual user accounts
- Compromise of individual user accounts
- Compromise of desktop systems
- Forgery, misrepresentation, or misuse of resources
- Loss of removable media or portable equipment

Incident Handling Process

Contain the Incident - *Prevent problems with affected areas from spreading*

- Identify and isolate the area under investigation
- Notify law enforcement personnel and legal services if applicable
- Notify communications team if necessary
- Document containment information

Eradicate the Incident - *Put an end to whatever caused the incident*

- Gather evidence
- Identify the source of the incident
- Determine the full extent of the incident
- Implement stopgap measures to eliminate any active threats
- Update documentation with eradication information

Recovery Process and Follow-Up

Assess damages - *Determine the impact of the incident to the council*

- Identify the affected systems and networks.
- Identify the affected data.
- Identify possible courses of remediation.

Reverse damages if possible - *Minimise the costs, both tangible and intangible, associated with the incident*

- Restore affected data from backup (if required)
- If necessary contact communications with regard to press release.

Nullify the source of the incident - *Prevent recurrence of the same incident*

- Patch any open vulnerabilities (if technical issues)
- Improve access restrictions to the affected areas
- Further remediation as necessary

Review the Incident - *Learn from the mistakes*

- Determine why the incident was able to occur.
- Determine if the appropriate safeguards are in place to prevent recurrence.
- Determine the risk level of similar incidents to other information assets.

Review the Incident Handling Plan - *Adapt and increase efficiency in the response process.*

- Validate that the incident handling and response plan was appropriate.
- Modify the incident handling and response plan with insight gained.

Documentation - *Keep tidy records, as they will almost certainly be needed again*

- Create final documentation of the incident in an appropriate level of detail.

- Perform debriefings if necessary.

  Risk Registers – The need to review and/or amend information systems, and Corporate Risk Registers.

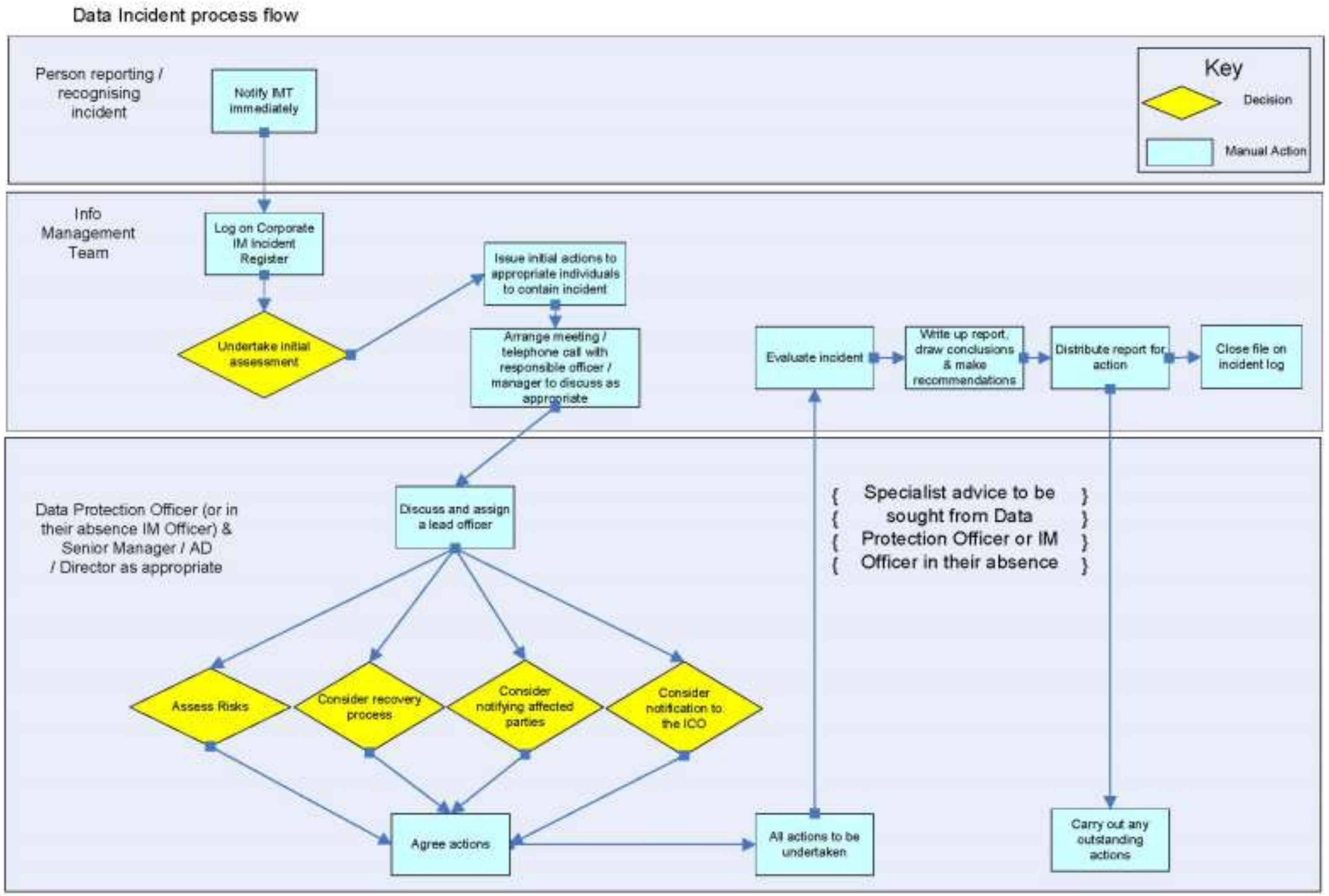
- Review all necessary risk registers to ascertain if amendments are required.

14. Appendix D – GovCertUK Incident Reporting

GovCertUK Incident Report

General Information	
Reported By:	**Date/Time Detected:**
Department:	**Date/Time Reported:**
Title:	**Mobile:**
Phone:	**Fax:**
Email Address:	**Additional Information:**
Postal Address:	
Incident Details	
Type of Incident:	
Status of the Department (total failure, business as usual etc):	**Classification of affected System:**
Incident Details:	
Site Details:	**Site Point of Contact:**
Actions Taken:	

15. Appendix E – Data Protection Incident Process Map


Data Incident process flow
Key
Decision
Manual Action
Person reporting / recognising incident
Notify IMT immediately
Info Management Team
Log on Corporate IM Incident Register
Undertake initial assessment
Issue initial actions to appropriate individuals to contain incident
Arrange meeting / telephone call with responsible officer / manager to discuss as appropriate
Evaluate incident
Write up report, draw conclusions & make recommendations
Distribute report for action
Close file on incident log
Data Protection Officer (or in their absence IM Officer) & Senior Manager / AD / Director as appropriate
Discuss and assign a lead officer
Specialist advice to be sought from Data Protection Officer or IM Officer in their absence
Assess Risks
Consider recovery process
Consider notifying affected parties
Consider notification to the ICO
Agree actions
All actions to be undertaken
Carry out any outstanding actions

16. Appendix F - Further contacts for IS Officers

LondonPSN can be contact in the following ways:

- General Communications / Enquiries email: office@londonpsn.gov.uk
- Orders emails: orders@londonpsn.gov.uk
- The LondonPSN Service Desk can be contacted in the following ways:
- Phone: **0845 845 5776**
- Support email: support@londonpsn.gov.uk
- Security Incidents email: incident@londonpsn.gov.uk
- Change Request email: change@londonpsn.gov.uk

The LondonPSN Service Desk operates Monday to Friday between 8am and 6pm excluding Bank Holidays. All phone calls outside of these times are answered by Virgin Media Businesses Fault Management Centre which is open 24 x 7 x 365

All emails sent outside of these times are picked up by the LondonPSN Service Desk during the next working day

PCI Contacts are

Barclaycard

Sarah Marlow

1234 Pavilion Drive

Northampton

NN4 7GS

United Kingdom

Email : Sarah.Marlow@barclaycard.co.uk

Tel: 01604 254042

WorldPay

Sade Haye

The Walbrook Building,

25 Walbrook

London EC4N 8AF

Tel 0203 664 5836 |

Email: Sade.Haye@worldpay.com>

17. Appendix G – Risk Management and Incident Reporting Process: Process Map