DBC '999' Personal Data Breach or Incident Reporting Procedure

Signed: Claire Hamilton **Chief Executive**

Number:	**DBC999 IS Proc**	**Title:**	**Personal Data Breach or Incident Reporting Procedure**				
Owner:	**IS Team Leader**	**Rev**	**4.2**	**Date**	**22nd December 2020**	**Classification**	**UNRESTRICTED**

Why do I need to report a breach?

The General Data Protection Regulation (GDPR) make it mandatory to report a Personal Data or Special Category Data Breach (formerly Sensitive Personal Data) to the Information Commissioners Office within 72 Hours.

This procedure is intended to identify the actions to be taken in event of a Personal Data breach, Special Category Data Breach or security incident and the persons responsible for taking the actions. There is an associated policy document outlining the information security incident management strategy adopted by Dacorum Borough Council (DBC900 IS – Incident Reporting Policy)

Scope

The scope to which this procedure relates is defined in the related policy document (DBC900 IS – Incident Reporting Policy)

Security Incidents can be either;

1. Technical (GDPR or Data Protection Breach {Personal Data breach or Special Category Data Breach}). ICT Virus / Malware, Information Security Policy Breach, Information Management Policy Breach, Retention Policy breach etc.)
2. Manual (Loss or breach of Paper records) – GDPR, UK Data Protection Act 2018, Freedom of Information Act, Records Management Policy)
3. Physical (Unauthorised Building or Site Access)

Categories

Breaches can fall into the following categories;

- Critical – Affecting all sites or > 1000 residents
- Major – Affecting one site / Group or 100 – 999 residents
- Medium – Affecting two or more members of staff or 10 – 99 residents
- Minor – Affecting one member of staff or 1-9 residents

NOTE: Virus / Malware infections, spam emails should initially be reported to ICT helpdesk who will log the call, and notify the Information Security Team Leader if the incident is serious.

Contact the ICT Service Desk; Ext 2234, DDI 01442 228234 or email ictservicedesk@dacorum.gov.uk

NOTE: In the event of a virus or malware infection, or other technical breach, ICT will not be held responsible for any loss of unauthorised software or personal files stored on a Council managed device.

Definitions

The definition of a “Security Incident” or “Breach” is an adverse event that has caused or has the potential to cause damage to an organisation’s assets, reputation and / or personnel.

Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

A Security Incident or breach includes, but is not restricted to, the following:

- The loss or theft of Personal Data, Special Category Data or information. (electronic or manual records).
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage on a Council network, system or database.
- Changes to information or data or system hardware, firmware, or software characteristics without the Council's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.

Examples of some of the more common forms of Security Incidents have been provided in Appendix 1

Outline of Approach

All incidents should be processed by addressing each of the following sections in the specified order. The sections are;

Record – initial recording of incident information

Investigate – Assess the scope and impact of the incident and effect ‘containment’

Resolve – Remedy the incident resulting in the affected users and equipment being placed back in ‘business as usual’ status.

Close – Conduct a post incident review

The remainder of this document describes each section in more detail including primary responsibilities.

Recording of the Incident (Responsibility: <u>All Staff</u>)

PLEASE REFER TO APPENDIX 2 FOR THE WORKFLOW OF HOW TO REPORT A SECURITY INCIDENT

It is the responsibility of all DBC employees including councillors to report any (suspected) Personal Data or information security incidents.

All incidents should be reported to your Line Manager and the Information Security Team Leader (Legal Governance);

E-mail john.worts@dacorum.gov.uk or Ext 2538, DDI 01442 228538 or in the absence of the Information Security Team Leader, Farida Hussain (Group Manager – Legal & Corporate Services) or Nargis Sultan (Barrister)

The Information Security Team Leader will record the breach or alleged breach, incident or suspected incident in the (suspected) incident in the GDPR Breach Register, generate a unique reference number and notify the reference number to the person reporting the incident, and depending on the severity.

The Information Security Team Leader will assess the incident to determine its classification (Critical, Major, Medium, and Minor). The Information Security Team Leader will contact the Assistant Director (Corporate & Contracted Services), Group Manager (Legal & Corporate Services) and may contact the Council's Corporate Anti-Fraud Unit, Human Resources or external bodies (such as the Information Commissioners Office, GovCerts UK).

Investigation (Responsibility: Information Security Team Leader

The Information Security Team Leader (Group Manager or other Legal Officer) has delegated responsibility from the Assistant Director (Corporate & Contracted Services) to assume primary responsibility for the investigation of all Personal data breaches, special category data breaches or information security incidents. The Assistant Director (Corporate & Contracted Services) will notify the relevant director that a breach or incident has occurred prior to formal notification to CMT.

Depending on the volume, severity and types of information breached, the Information Commissioner will be notified.[1]

The Information Security Team Leader will necessarily need to involve other parties, both within the Council and possibly externally.

The Information Security Team Leader will assess the following (all steps must be documented);

The scope and nature of the breach or incident.

Review all available evidence and information in relation to the breach or incident (for example, paper records, emails, computer logs, internet logs, email logs and server logs)

Dependent on the nature of the breach or incident it may be necessary to preserve the incident scene for evidential purposes. For example, it may be necessary to perform a data backup of computer-related information before taking any action to resolve the incident.

[1] For more information – please see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

There may be a requirement depending on the nature of the breach or incident to suspend or disable network accounts (including remote access) and system wide accounts, plus any physical building access. This will only be done by authorisation from the relevant line manager.

There may be a need to contain the incident, that is, prevent the incident from spreading to more users, systems, applications or devices. Typically this will be the case in the event of a computer virus attack. Containment may consist of actions in one or more of the following areas; Staff notification/assistance, disablement of services or (network) disconnection. Any modifications should always adhere to the ICT Change Management process where appropriate.

The Information Security Team Leader will communicate regularly with all stakeholders to provide a status report on the incident.

Resolution (Responsibility: Solicitor to the Council / Investigation Team Members / Information Security Team Leader)

Having possibly preserved evidence of the incident and taken steps to contain any spread there will be a need to resolve the incident such that users, systems or devices are returned to their usual operational state.

Depending on the nature of the incident it may be necessary to re-build the configuration of the device(s) from a known good data backup or software image. Alternatively the remedy may involve the use of anti-virus software or other technological solutions. The Information Security Team Leader will advise on the most appropriate course of action having consulted with in-house and possibly external experts. Any modifications should always adhere to the ICT Change Management process where appropriate.

Where remedial action has been taken in respect of breach or loss of Personal Dara or Special Category Data, this will be recorded along with any solution to strengthen the procedure.

The Information Security Team Leader will communicate regularly with all stakeholders to provide a status report on the incident.

Close

When it has been determined that the incident has been successfully resolved the Information Security Team Leader will complete the breach or incident documentation and close the corresponding incident record in the Councils GDPR Breach Register.

All internal and external stakeholders will be informed by the Solicitor to the Council or nominated investigation team members of the resolution of the breach or incident.

The Information Security Team Leader should arrange a post completion review to ascertain any lessons learned from the incident and where appropriate generate actions to reduce the likelihood of recurrence. For example, there may be a need to apply software patches to resolve vulnerabilities.

It is critical that the nominated investigation team members compiles and securely retains full documentation relating to the incident so that any lessons may be learned or to support subsequent legal action.

Supporting Documentation

DBC900 IS Information Security Incident Policy

DBC001 IS Corporate Information Security Management Policy

DBC010 IS Corporate Information Technology Security Policy

DBC100 IM GDPR / Data Protection Act 2018 Policy

Appendix 1 – Examples of Information Security Incidents and Breaches

Examples of the most common Information Security breaches or incidents are listed below. It should be noted that this list is not exhaustive.

Remember – a breach or security incident can be either electronic or manual (paper based) or a combination of both.

- Personal Information being sent out to the wrong address. Note: be very careful with email addresses and 'autocomplete'. Ask the data subject to send you an email initially so that you can respond to the correct email address.
- Employee has a laptop stolen after being left in car boot overnight!
- Sensitive Information being left on printer tray in a corridor unattended
- Personal or Sensitive Personal information being left unattended on a desk or screen (shoulder surfing)
- Lack of security around personal or sensitive personal data e.g. Personal Information being dumped in a public waste bin / skip
- Information being processed for another purpose
- Information being destroyed prematurely or kept too long
- Giving information to someone who should not have access to it - verbally, in writing or electronically.
- Sending a sensitive e-mail to 'all staff' by mistake
- Unauthorised modification of (personal) data or information
- Introduction of virus / malware

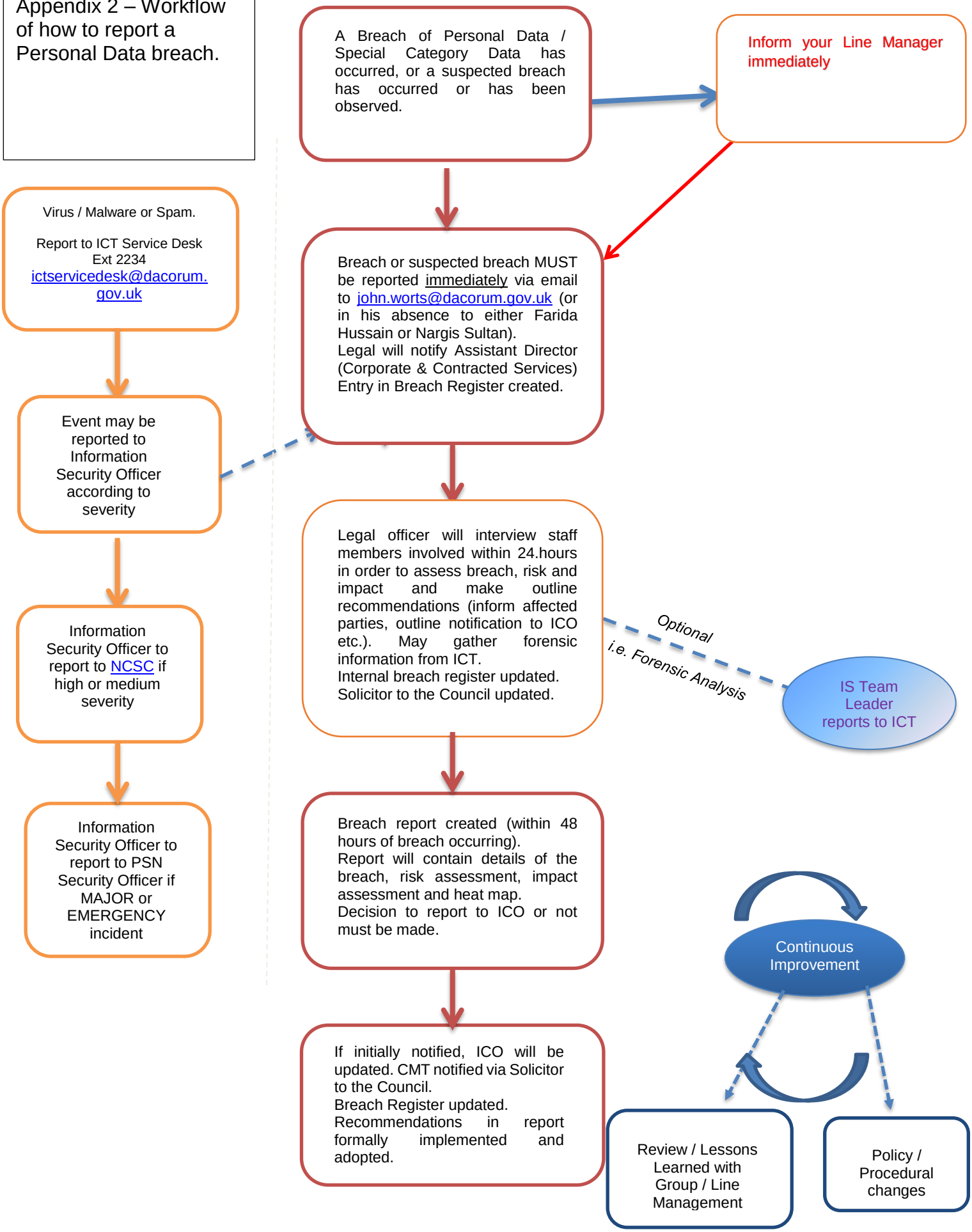
Misuse

- Use of unapproved or unlicensed software on Dacorum Borough Council equipment.
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password).
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.

Theft / Loss

- Loss of Personal Data / Special Category Data
- Compromise of Personal Data / Special Data
- Theft / loss of a hard copy file.
- Theft / loss of any Dacorum Borough Council computer equipment
- Sending information to an unintended recipient.

Appendix 2 – Workflow of how to report a Personal Data breach.



Document Control

Author:	John Worts - Information Security Team Leader
Owner:	Mark Brookes – Solicitor to the Council (Legal Governance)
Document Number	V4.2

Revision History

Revision Date	Previous Revision Level	Summary of Changes	Next Review Date
18/4/12	1.0	Change of document number and title in alignment with policy and procedure refresh. Change contact details. Added 'Definitions', Appendix 1 – Examples & Appendix 2 – Workflow	April 2013
21/6/12	2.0	Added in information specifically to manual (paper) records	June 2013
29/6/12	2.1	Reporting workflow changed, and document structure changed to make reporting easier. Title changed to Incident Reporting Procedure.	June 2013
5/7/12	2.2	Added in note for ICT specific incidents. Minor amendments post CMT review	July 2013
11/7/12	2/3	CMT Approved FINAL	July 2013
12/9/12	2.4	Revised to incorporate new reporting structures and notification to ICO	Sept 2013
5/7/13	2.5	Review by Infrastructure Team leader. Malware / Virus reporting clearer, and added in report to GOVCERTS	July 2014
18/9/13	2.6	Aligns with Helpdesk procedure	Sept 2014
15/6/14	2.8	Added PSN and definitions	June 2015
8/1/15	2.8	Change to title to include breach and escalation to CMT in Appendix 2	Jan 2016
18/7/17	2.9	Changes to reporting body (NCSC) and updates to new ICT Helpdesk email address and owning officer.	July 2018
23/4/18	3.0	Major Overhaul for GDPR	April 2019
13/1/20	4.0	Revisions to GDPR and DPA. Clarity of scope of breach	January 2021
22/12/20	4.1	Changes to Job Titles and added in 'breach' to portions of the document	December 2021