sustainable thriving achieving
East Dunbartonshire Council
www.eastdunbarton.gov.uk

Security Incident Theft or Loss Reporting and Recording Procedures

Version Control

Author:	Iain Stewart
Owner: (This field must specify the senior responsible officer and their department)	Vince McNulty – ICT Manager
Source Location:	Z:\ public \\Legacy-VS\Legacy\ICT-Policies
Other Documents Referenced:	
Related Documents:	Security incident Reporting & Management Mobile Device Policy
Contact:	Iain Stewart Iain.stewart@eastdunbarton.gov.uk or iain.stewart@eastdunbarton.gsx.gov.uk 0141 578 8035 07766424497

Change History

This document is subject to change control and any amendments will be recorded below.

Version	**Date**	**Changes**	**Author**	**Authorised**
0.1	14/11/2012	Initial draft	IS (EDC)	
0.1a	15/11/2012	Draft Wording review and changes by Jim McCallum	IS (EDC)	JM (EDC)
0.1b	19/11/2012	Draft Addition of GovCert url – 3.2.4	IS (EDC)	IS (EDC)
0.1c	08/04/2013	Additional of sign off section within Appendix A, Contact email updated, document source location updated	IS (EDC)	

Version Awareness

This document may not be the latest available version. The latest version, which supersedes all previous versions, is available at: <LINK>

1 Introduction

This document and the Incident Review Data Sheet (Appendix A) should be used to determine the procedure to follow, timescales, responsibilities and information required in order to report and record a lost or stolen ICT device belonging to East Dunbartonshire Council.

ICT define a device as any item that can hold electronic data such as but not exclusively a mobile phone, Blackberry, USB Flash Drive, Memory Cards, Laptop, Tablet or PC

1.1 Scope

This procedure is designed to ensure robust recording, reporting and reporting whilst preventative measures are taken to manage and minimise risk associated with a lost or stolen ICT device.

This procedure is designed for ICT staff use as a mandatory recording tool. It may also provide end users of ICT with insight into the required processes and information requirements following the loss or theft of an ICT device.

2 Incident Reporting

2.1 Incident reporting

As outlined within East Dunbartonshire mobile device policy, the loss of any Council-owned device must be reported to the appropriate line manager and also to the ICT Service Desk where possible within one working day.

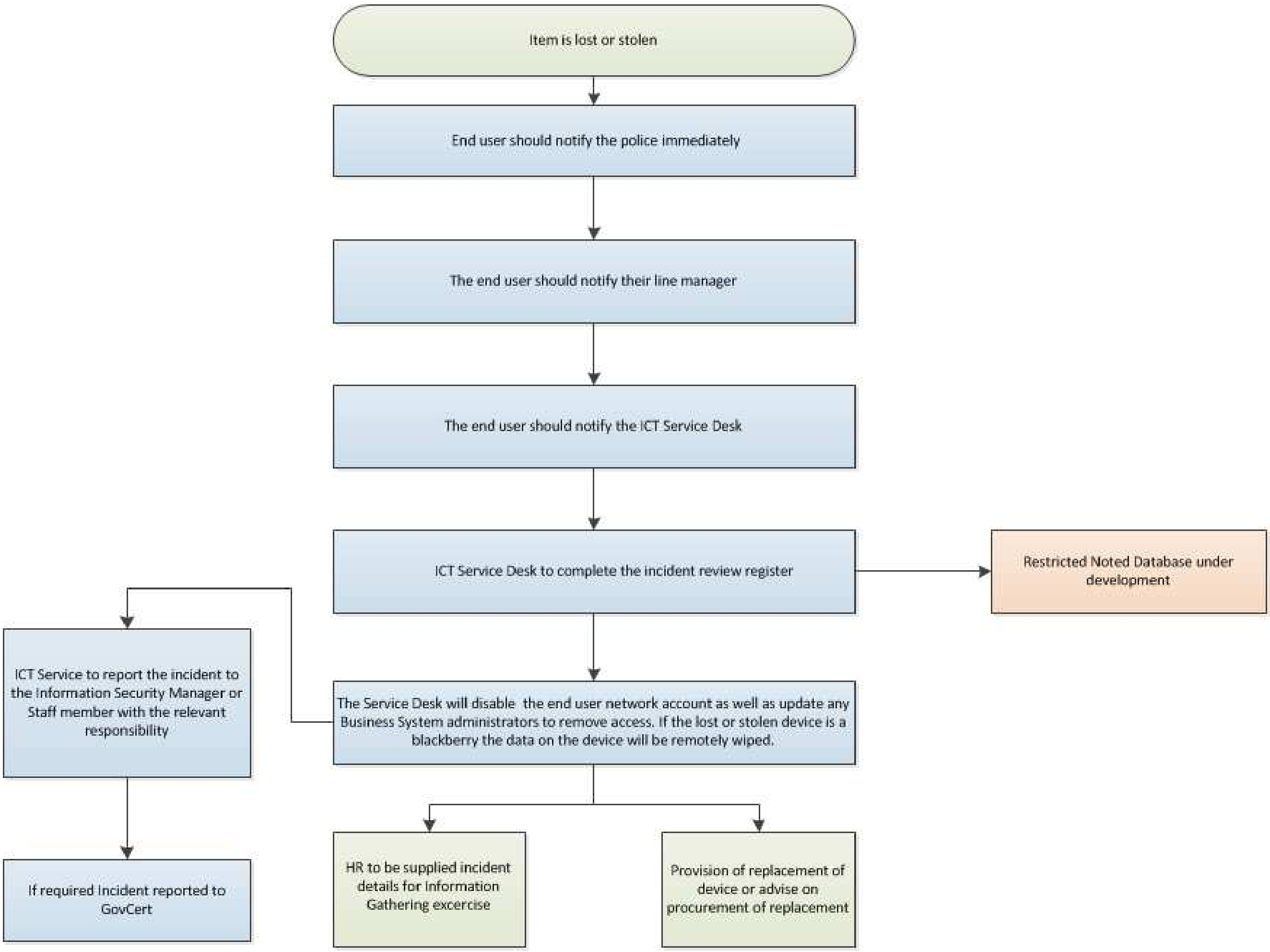
If a Council ICT device is lost or stolen, the sensitivity of the lost information should be assessed, in accordance with the Incident Investigation Procedure, to determine the potential impact on members of the public, employees and the Council’s reputation. Any mitigating actions can then be assessed and implemented. This impact assessment must be undertaken within 24 hours following the loss or theft being reported.

Loss or damage to, Council-owned portable computers will be investigated in accordance with the Incident Investigation Policy. Where negligence on behalf of the custodian has resulted in the loss or damage disciplinary action may be taken in accordance with Council procedures. Any instance of negligence will be investigated by Customer Services & Transformation.

3 Process of Reporting

3.1 Process of Recording

When a device is reported as being lost or stolen to the ICT Service Desk the following charts outline the procedure that will be followed to ensure all the required information is recorded and any required preventative measures are taken to reduce risk


Item is lost or stolen
End user should notify the police immediately
The end user should notify their line manager
The end user should notify the ICT Service Desk
ICT Service Desk to complete the incident review register
Restricted Noted Database under development
ICT Service to report the incident to the Information Security Manager or Staff member with the relevant responsibility
The Service Desk will disable the end user network account as well as update any Business System administrators to remove access. If the lost or stolen device is a blackberry the data on the device will be remotely wiped.
If required Incident reported to GovCert
HR to be supplied incident details for Information Gathering excercise
Provision of replacement of device or advise on procurement of replacement

3.2 Time Scales for Reporting

3.2.1 End User

Once a device has be identified as lost or stolen, the end user must report this to the police immediately and to their line manager as soon as possible, time scales for end users are outlined within both the Acceptable use Policy and the Mobile Device Policy.

The end user or their line manager should then report the incident to the ICT Service Desk as per timescales outlined within both the Acceptable use Policy and the Mobile Device Policy.

3.2.2 ICT Service Desk and ICT Support Staff

The ICT Service Desk will record the relevant details on the Incident Review Data Sheet (Appendix A) at time of taking the call; the Incident Review Data Sheet should be completed with all the relevant information to ensure a timely resolution.

3.2.3 ICT Service Desk Tasks

A service desk call should be logged for the following

- If the lost or stolen device is a computer such as a laptop, tablet or desktop PC. A Priority 1 call should be logged to have the end users Network password reset for Novell as well as any remote access solution currently in place (e.g. AppGate / Portal) The Service Desk will also contact any relevant System Administrators to alert them to the incident and ensure any system specific assess is reset.

- If the lost or stolen device is a Blackberry mobile a Priority 1 call should be logged and assigned to an appropriate ICT Support Team member who should also be alerted by telephone to undertake a remote wipe of the device within 1 hour. The Service Desk will liaise with the department involved to discuss a replacement. At present due to costs ICT do not hold spare Blackberry devices.

- If the lost or stolen device is a computer a priority 2 call should be logged in order for a replacement to be provided to the end user to allow normal day to day duties to be undertaken.

The ICT Service Desk will forward a copy of the Incident Review Data Sheet (Appendix A) to the Information Security Officer within 1 hour and also alert them by telephone to inform them of the Incident.

3.2.4 Information Security Officer

The information Security Officer or relevant member of ICT staff should report the Incident details to the ICT Management Team within 1 working day.

The Information Security Officer or relevant member of ICT staff should also report the Incident to CST within 2 working days and if required pass any relevant information within 4 working days for any Information Gathering / Fact finding exercise.

When and where required the incident should be reported to both GovCert and the Socitm Security Group as per GSX Code of Connections requirements. This should take place no more than 5 working days after the initial reporting of the incident.

Assistance of incident classification and categorisation can be found at the following url

http://www.cesg.gov.uk/policyguidance/GovCertUK/Pages/index.aspx

3.2.5 Customer Services & Transformation responsibilities

CST will undertake any information gathering process, the Information Security Officer may be called as a witness to this process, to determine any further action required, this could be in the form of one or more of the following

- Reminder of Council Policies
- Disciplinary Action

This process should be complete and results passed to ICT to allow the closure of the Incident within the Security Incident Database by the Information Security Officer.

sustainable thriving achieving
East Dunbartonshire Council
www.eastdunbarton.gov.uk

Appendix (a) – Incident Review Data Sheet.

General Information			
Details Record by (IT Staff)		SD Ref	
Full Name (end user)			
Department		Base Location	
Contact Email			
Telephone Number(s)			
Line Manager Name			
Current Time		Current Date	
Incident Information			
Description Of Incident			
Date of Incident		Time of Incident	
If Applicable, details of where Item was stolen from, e.g. locked office, open office, unlocked storage cupboard, car back seat, car boot, home, coffee shop			
If Applicable was the area, locked or alarmed (car or home), covered by CCTV, accessible by multiple people (supply names if possible)			
Address Incident Occurred			
When was the Item last seen or used? Approximate date & time			

If Applicable			
Police Incident No.			
Police Crime No.			
Station Reported to			
Officer Name			
Date reported		Time Reported	
Security Questions			
Where any user or system passwords taken with the device, stored or record on the device or in paperwork that may have been taken? If yes provide details of each			
If a computer device, did the machine contain any restricted or confidential information relating to EDC business, members of staff, members of the public or information that could cause reputational damage if released to the general public?			
Was any paperwork or USB pen drives taken that may continue information as above?			
If USB Pen Drive, was it EDC approved Encrypted device?			
If the device was a mobile phone please confirm the number			
If a mobile phone did the device have a pin or security code?			
Which make and model was the mobile phone?			
Where any other EDC items taken, such as ID badge, computer peripherals, keys?			

sustainable thriving achieving
East Dunbartonshire Council
www.eastdunbarton.gov.uk

Asset Information : Source details from FrontRange , WASP or Blackberry BES			
Complete as applicable			
Item Type			
Make		Model	
Serial Number		Asset Tag	
Last Check In Time			
Last Check in User			
Last Check in IP address			
Information may be sourced from Purchasing or Supplier			
Purchase Date		Purchase Price	
Replacement Price			

Confirmation And Sign Off	
I confirm the information provided within Appendix A is accurate and true reflection	
Employee Name	
Employee Signature	
Date	

Manager Sign Off	
Manager Name	
Manager Signature	
Date	