Information Security Incident Protocol

Document Owner	Caroline Dodge Tel: 01622-221652 caroline.dodge@kent.gov.uk
Version	Version 2: July 2013

Contents

1. Protocol Objectives
2. Scope
3. Protocol Statement
4. In the event of a suspected breach
5. Non-compliance with protocol
6. Assistance and guidance
7. Definitions
8. Appendix A -
9. Appendix B

1. Protocol Objectives

Any information that could identify a living individual is classed as personal data. All data subjects have a right to access their own personal data that is held by KCC as Data Controller. Consequently, KCC can be considered to be the ‘custodian’ of that information and has, therefore, the responsibility of ensuring its confidentiality.

KCC is committed to ensuring the security and integrity of that information by implementing and maintaining appropriate controls and procedures for handling and storing of personal and sensitive information. KCC has, therefore, the responsibility of taking appropriate steps in the event of the loss, theft or uncontrolled exposure of personal or sensitive information for which it is the custodian.

This protocol sets out the steps that must be followed in the event of loss, theft or uncontrolled exposure of personal or sensitive information for which KCC has responsibility.

2. Scope of this Protocol

The protocol applies to all KCC staff and volunteers and, through contractual arrangements to KCC, suppliers, partners, contractors, agents, consultants and commissioned services, in the course of functions carried out for or on behalf of KCC.

Members (elected Councillors) have similar responsibilities. These are set out in the Members’ Code of Conduct.

Throughout this document the word ‘*information*’ refers to information that relates to personally identifiable individuals (as is defined within the Data Protection Act) or is commercial or political information of a sensitive/confidential nature.

Computerised equipment, for the purposes of this protocol, includes, but is not limited to: personal computers (PCs – laptops, notebooks, tablets and palmtops); application servers, file/print servers; Personal Digital Assistants (PDAs); Blackberries and mobile phones. It also includes all types of: removable storage media; peripheral devices and; accessories physically attached, or connected by wireless networks, to the computerised equipment.

3. Protocol Statement

Anyone who handles personal or sensitive information for and/or on behalf of KCC must:

- take all reasonable steps to ensure the security of that information to minimise the risk of an information security breach, including the loss of personal or sensitive information;

- follow the procedure outlined below in the event of any breach of security.

4. In the event of a suspected information security breach:

DO NOT WAIT – ACT and REPORT ANY INCIDENTS IMMEDIATELY

It is crucial to act quickly in the event of a suspected information security incident, in order to minimise the impact of the incident and safeguard the privacy of individuals as far as possible and minimise the risk to KCC.

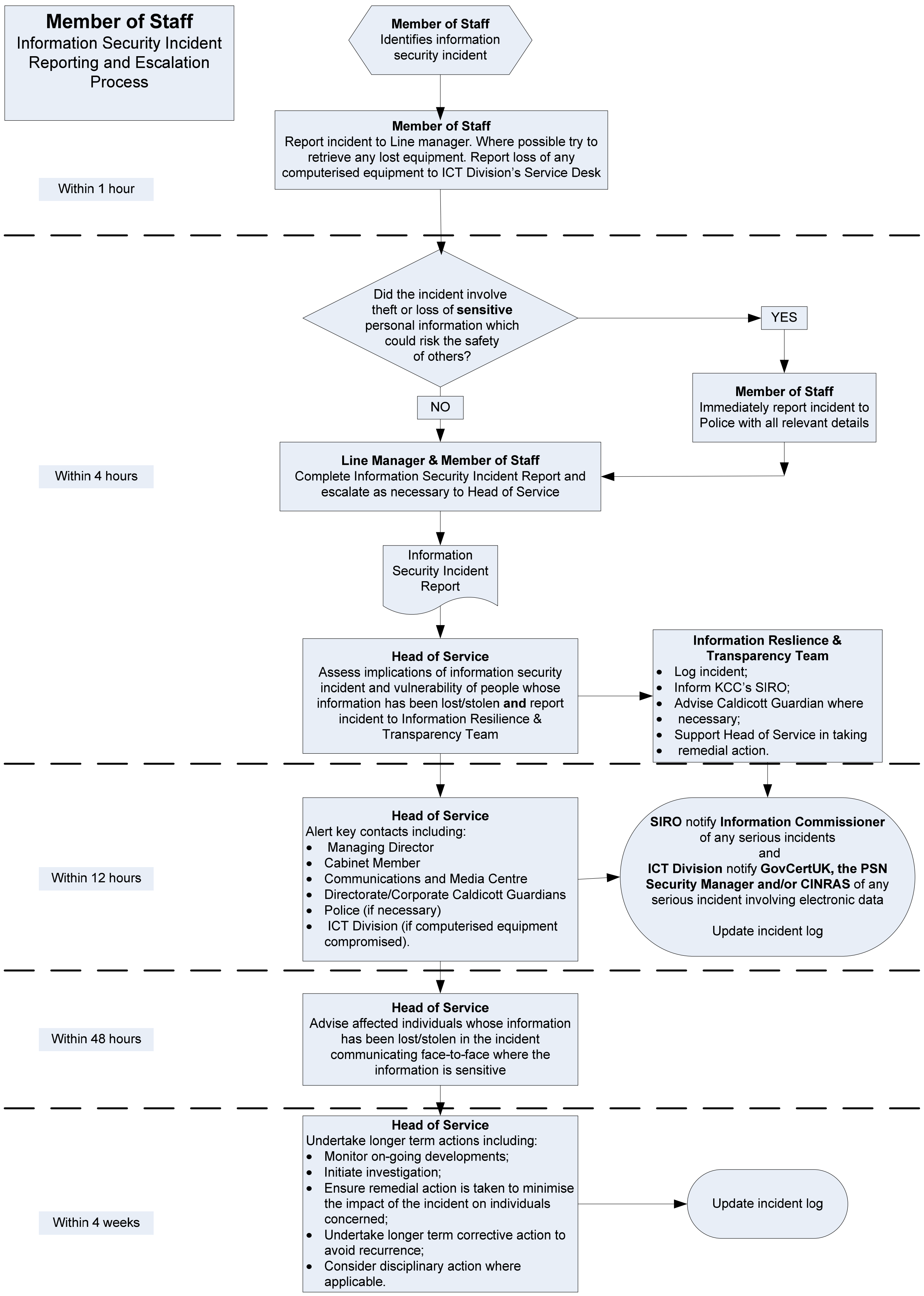
The initial steps that should be taken to alert managers about an incident will vary depending on whether the incident involved a member of KCC staff, a supplier or commissioned service, a service user or a member of the public.

The flow charts and supporting sections in this document set out the steps that should be followed in the event of an information security incident for each of these three circumstances:

- A member of KCC staff or a Member or a volunteer identifies a potential information security incident;
- A supplier or provider of commissioned services identifies and reports a potential information security incident;
- A service user or a member of the public identifies and reports a potential information security incident.

Member of Staff

Information Security Incident Reporting and Escalation Process



Member of Staff
Identifies information security incident

Within 1 hour

Member of Staff
Report incident to Line manager. Where possible try to retrieve any lost equipment. Report loss of any computerised equipment to ICT Division's Service Desk

Did the incident involve theft or loss of **sensitive** personal information which could risk the safety of others?

YES

Member of Staff
Immediately report incident to Police with all relevant details

NO

Within 4 hours

Line Manager & Member of Staff
Complete Information Security Incident Report and escalate as necessary to Head of Service

Information Security Incident Report

Head of Service
Assess implications of information security incident and vulnerability of people whose information has been lost/stolen **and** report incident to Information Resilience & Transparency Team

Information Reslience & Transparency Team
- Log incident;
- Inform KCC's SIRO;
- Advise Caldicott Guardian where
- necessary;
- Support Head of Service in taking
- remedial action.

Within 12 hours

Head of Service
Alert key contacts including:
- Managing Director
- Cabinet Member
- Communications and Media Centre
- Directorate/Corporate Caldicott Guardians
- Police (if necessary)
- ICT Division (if computerised equipment compromised).

SIRO notify **Information Commissioner** of any serious incidents
and
ICT Division notify **GovCertUK, the PSN Security Manager and/or CINRAS** of any serious incident involving electronic data

Update incident log

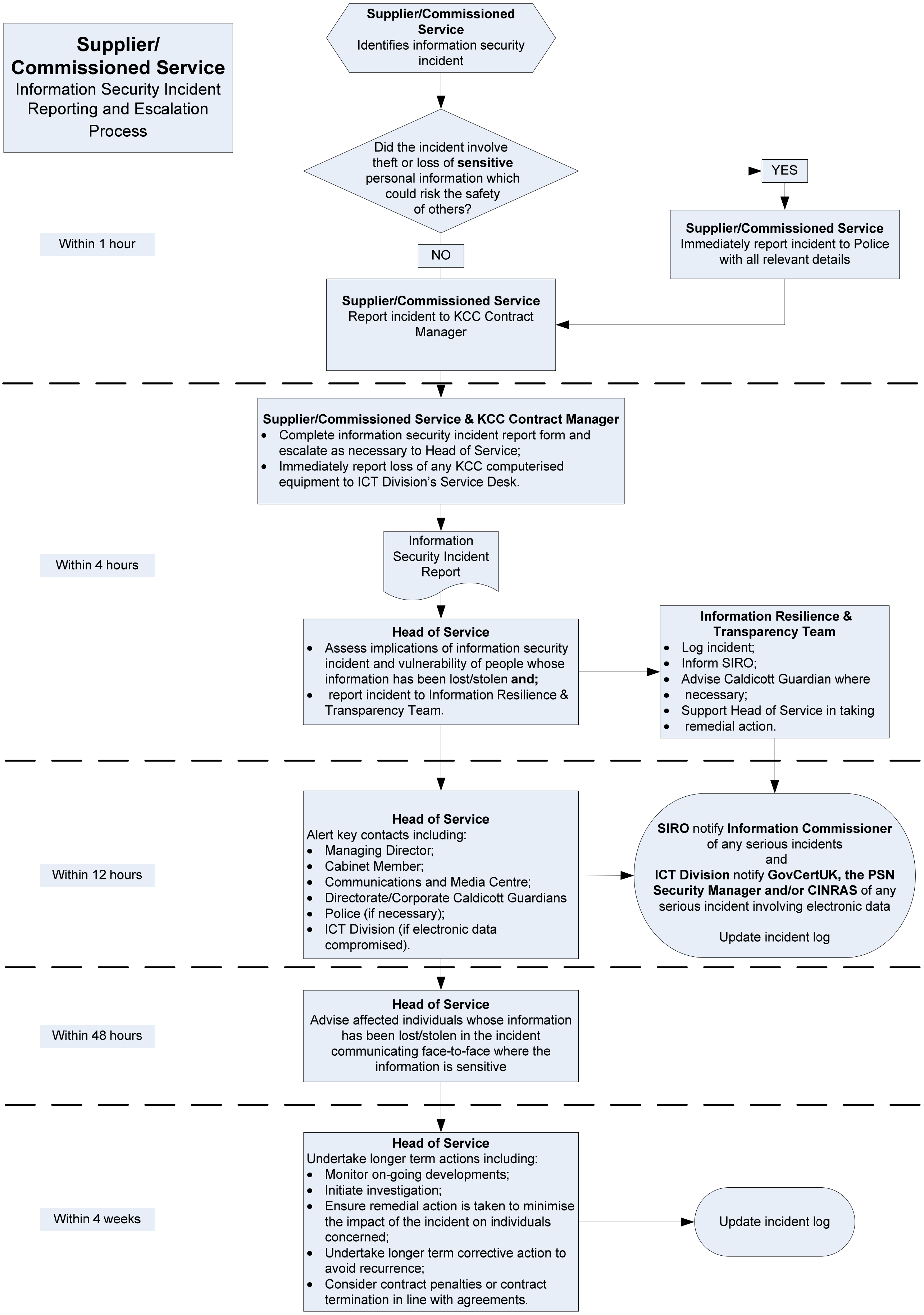
Within 48 hours

Head of Service
Advise affected individuals whose information has been lost/stolen in the incident communicating face-to-face where the information is sensitive

Within 4 weeks

Head of Service
Undertake longer term actions including:
- Monitor on-going developments;
- Initiate investigation;
- Ensure remedial action is taken to minimise the impact of the incident on individuals concerned;
- Undertake longer term corrective action to avoid recurrence;
- Consider disciplinary action where applicable.

Update incident log



Supplier/ Commissioned Service

Information Security Incident Reporting and Escalation Process

Supplier/Commissioned Service
Identifies information security incident

Did the incident involve theft or loss of **sensitive** personal information which could risk the safety of others?

YES

Supplier/Commissioned Service
Immediately report incident to Police with all relevant details

NO

Within 1 hour

Supplier/Commissioned Service
Report incident to KCC Contract Manager

Supplier/Commissioned Service & KCC Contract Manager

- Complete information security incident report form and escalate as necessary to Head of Service;
- Immediately report loss of any KCC computerised equipment to ICT Division's Service Desk.

Information Security Incident Report

Within 4 hours

Head of Service

- Assess implications of information security incident and vulnerability of people whose information has been lost/stolen **and;**
- report incident to Information Resilience & Transparency Team.

Information Resilience & Transparency Team

- Log incident;
- Inform SIRO;
- Advise Caldicott Guardian where
- necessary;
- Support Head of Service in taking
- remedial action.

Within 12 hours

Head of Service
Alert key contacts including:

- Managing Director;
- Cabinet Member;
- Communications and Media Centre;
- Directorate/Corporate Caldicott Guardians
- Police (if necessary);
- ICT Division (if electronic data compromised).

SIRO notify **Information Commissioner** of any serious incidents
and
ICT Division notify **GovCertUK, the PSN Security Manager and/or CINRAS** of any serious incident involving electronic data

Update incident log

Within 48 hours

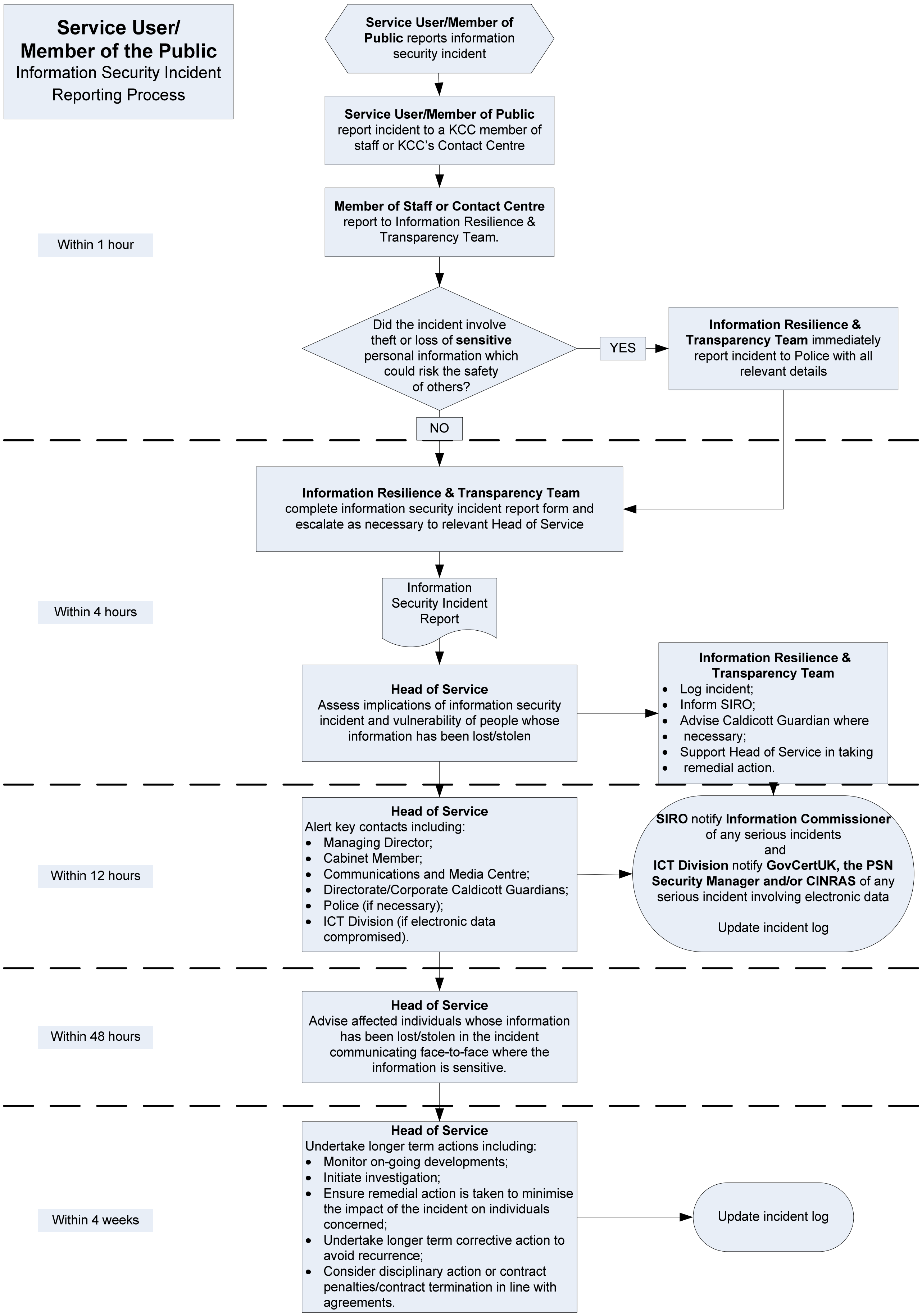
Head of Service
Advise affected individuals whose information has been lost/stolen in the incident communicating face-to-face where the information is sensitive

Within 4 weeks

Head of Service
Undertake longer term actions including:

- Monitor on-going developments;
- Initiate investigation;
- Ensure remedial action is taken to minimise the impact of the incident on individuals concerned;
- Undertake longer term corrective action to avoid recurrence;
- Consider contract penalties or contract termination in line with agreements.

Update incident log



Service User/ Member of the Public
Information Security Incident Reporting Process

Service User/Member of Public reports information security incident

Service User/Member of Public report incident to a KCC member of staff or KCC's Contact Centre

Within 1 hour

Member of Staff or Contact Centre report to Information Resilience & Transparency Team.

Did the incident involve theft or loss of **sensitive** personal information which could risk the safety of others?

YES

Information Resilience & Transparency Team immediately report incident to Police with all relevant details

NO

Information Resilience & Transparency Team complete information security incident report form and escalate as necessary to relevant Head of Service

Within 4 hours

Information Security Incident Report

Head of Service
Assess implications of information security incident and vulnerability of people whose information has been lost/stolen

Information Resilience & Transparency Team
- Log incident;
- Inform SIRO;
- Advise Caldicott Guardian where
- necessary;
- Support Head of Service in taking
- remedial action.

Within 12 hours

Head of Service
Alert key contacts including:
- Managing Director;
- Cabinet Member;
- Communications and Media Centre;
- Directorate/Corporate Caldicott Guardians;
- Police (if necessary);
- ICT Division (if electronic data compromised).

SIRO notify **Information Commissioner** of any serious incidents and **ICT Division** notify **GovCertUK, the PSN Security Manager and/or CINRAS** of any serious incident involving electronic data

Update incident log

Within 48 hours

Head of Service
Advise affected individuals whose information has been lost/stolen in the incident communicating face-to-face where the information is sensitive.

Within 4 weeks

Head of Service
Undertake longer term actions including:
- Monitor on-going developments;
- Initiate investigation;
- Ensure remedial action is taken to minimise the impact of the incident on individuals concerned;
- Undertake longer term corrective action to avoid recurrence;
- Consider disciplinary action or contract penalties/contract termination in line with agreements.

Update incident log

5. Non-compliance with this Protocol

Failure to comply with this Protocol by:

- KCC employees: may result in disciplinary action and may, in cases of Gross Misconduct (including negligence or deliberate non-compliance), result in termination of employment;
- KCC Members: may be referred to the Standards Committee, which can recommend disciplinary measures to the Council;
- Third-Parties (agents, contractors and consultants) engaged to carry out work for and on behalf of Kent County Council: may result in the termination of the contract and/or litigation.

6. Assistance and Guidance

If you do not understand this Protocol or if you need clarification or more details regarding any of its points then contact KCC's:

- Information Resilience and Transparency Team; informationgovernance@kent.gov.uk
- Information Systems Security Officer, ICT Division, Business Strategy & Support;
- Senior Information Risk Owner, Governance & Law, Business Strategy & Support.

7. Definitions and additional information

'Information' takes many forms and includes information printed or written on paper (including photocopies and faxes), stored electronically (e.g. on computers or networked storage, disk media, digital tape, memory cards or sticks), transmitted by post or using electronic means, images, stored negatives, prints, slides, tape or video, spoken in conversation or via telephone.

'**Personal information**' is information about an identifiable individual as defined in the Data Protection Act 1998.

'**Sensitive information**' is information that if lost, stolen or inappropriately disclosed would adversely affect the privacy or safety of an individual, or harm the business interests or reputation of KCC or third parties.

A '**Security Incident**' is awareness of the possibility or actuality of a breach of security. This can take many forms, e.g. unauthorised access to, or the loss or theft of, KCC computerised equipment; the mislaying of a client's manual case file or the inappropriate disclosure of information (verbally, in writing or electronically) to someone who has no right or need to access it.

Examples of Information security incidents which would need to be reported include:

- Overhearing of confidential information;
- Unauthorised access to KCC computerised equipment;
- Loss of KCC computerised equipment.

Examples of more serious breaches which will require immediate remedial action include:

- Loss of one or more confidential case files;
- Email containing personal or sensitive information sent to the wrong email address;
- Fax containing personal or sensitive information sent to wrong fax number;
- Loss of KCC computerised equipment containing personal or sensitive information.

'Loss' – In the event of the item being knowingly lost as opposed to stolen, all of the above applies except that the Police will not report a crime and cannot issue a crime number.

'Lost and Stolen' – applies to hard copy information as well as computerised equipment, e.g. file left in a vehicle or on public transport or stolen with car or snatched in a bag, etc. Also applies to any personal details or sensitive information passed to an unauthorised individual in any manner or overheard by an unauthorised individual during a conversation.

Confirming, assessing and evaluating the situation may take at least 48 hours before being able to contact the affected person(s) or organisation(s) and may be heavily impacted upon if over a weekend. However, management are strongly advised to contact the affected persons at the earliest opportunity when facts are known. A sensitive, short but accurate letter must be sent with contact information for anyone who may be affected by the loss or disclosure of the information.

In some circumstances, service users are vulnerable adults and children and being informed of the security breach may be alarming. In these circumstances, the Corporate Director or their nominated deputy will consider appropriate communication strategies. It may be important to point out that at this early stage there is no indication that their personal security has been breached but the member of the public must remain vigilant and will be advised of any change in security status. If any of the information relates to personal finance details then the individual should be advised to contact their bank or building society urgently and to monitor their bank/building society account(s).

The Corporate Director or nominated deputy will need to prepare a briefing for all the necessary parties within a single email, copied to the appropriate contacts. Depending upon the potential seriousness of the security breach, contact is advised by phone as well as face to face. Any significant change to status will require follow-up communication.

The incident must remain in the '*OPEN*' status, until finally resolved and only '*CLOSED*' after it has been resolved, reviewed and any

requirements for training, disciplinary and/or procedural changes have been identified. As well as *OPEN/CLOSED* it is recommended that the incident has a traffic light (*Red – Amber – Green*) status which is reviewed regularly, both through any information governance and directorate risk management procedures.

Appendix A: - Document Version Control

Review History

Review Date	**Reviewed By**	**Changes Necessary ?**
25th July 2013	A.J. Cordina	Yes

Revision History

Revision Date	**Revision**	**Summary of Changes**
25th July 2013	V 1.0	To reflect PSN CoCo requirements.

Approvals

Name	**Title**	**Date of Issue**	**Version**

Appendix B: Distribution and disclosure of this document and its contents

The contents of this document have been given the '*UNCLASSIFIED*' category under HMG's 'National Protective Marking Scheme'.

The National Protective Marking Scheme (often referred to as the Government Protective Marking System/Scheme or GPMS) is Her Majesty's Government's administrative system to ensure that access to information and other assets is correctly managed and safeguarded to an agreed and proportionate level throughout their lifecycle, including creation, storage, transmission and destruction. The system is designed to support government business and meet the requirements of relevant legislation, international standards and international agreements.

The Protective Marking System comprises five markings. In descending order of sensitivity they are: *TOP SECRET*, *SECRET*, *CONFIDENTIAL*, *RESTRICTED*, *PROTECT* and *UNCLASSIFIED*.

These markings can be applied to any government assets, although they are most commonly applied to information held electronically or in paper documents.

For Local Authorities, such as Kent County Council, the protective markings which will be most commonly seen in the workplace are *UNCLASSIFIED*, *PROTECT* and *RESTRICTED*. Out of these it is anticipated that *UNCLASSIFIED* and *PROTECT* will be the most common.

‘*Unclassified*’ documents have no classification requirements and, therefore, must not include personal, confidential or sensitive information. ‘*Unclassified*’ documentation is that which includes terms of reference, minutes from open meetings, policies etc. and can, therefore, be placed into the public domain or published on the Internet.