APPENDIX 1

Peterborough City Council

Data Incident Response Policy

1.1. Policy Statement

Peterborough City Council holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

1.2. Purpose

This policy sets out the procedure to be followed by all Peterborough City Council Officers and Members if a data protection, including credit card/debit card, breach takes place.

1.3. Scope

This policy applies to all personal and sensitive data, including credit card/debit card details, held by Peterborough City Council.

1.4. Legal Context

The Data Protection Act 1998 makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

Principle 7 of the Data Protection Act 1998 states that organisations which process personal data must take "appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

1.4.1. Data

Data means information which –

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68 of the Data Protection Act 1998, or
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

1.4.2. Personal Data

Personal data means data which relates to a living individual who can be identified –

(a) from that data, or
(b) from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

1.4.3. Sensitive Personal Data

Sensitive personal data means personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,
(b) his/her political opinions,
(c) his/her religious beliefs or other beliefs of a similar nature,
(d) whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his/her physical or mental health or condition,
(f) his/her sexual life,
(g) the commission or alleged commission by him/her of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.
(i) Credit card/debit card details pertaining to the data subject

1.5. Types of Breach

Data protection breaches could be caused by a number of factors. Some examples are (this list is not definitive):

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as fire or flood
- Hacking
- 'Blagging' offences where information is obtained by deception

2. Breach Management

As soon as the data breach occurs or is discovered, it should be reported by whoever has committed or discovered the breach to their manager and the Head of Governance. The Head of Governance will then launch an investigation into the data breach including appointing a designated Investigation Lead Officer (ILO) who will be responsible for all aspects of the breach management process.

2.1. Containment and Recovery

The ILO will:

- Establish if the breach is ongoing and take immediate action to stop the breach and to minimise the impact and effect of the breach;
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise;
- Establish whether there is anything the Council can do to recover any losses and limit the damage the breach can cause;
- Instigate the recovery of physical equipment, where appropriate;
- As far as is practically possible, ensure that Council staff recognise when someone tries to use the lost or stolen data to access accounts;
- Inform the police, where appropriate;
- Inform the banks/building societies and card providers if appropriate: and
- Inform the Head of Communications so that a press statement can be prepared in the event of a media enquiry; depending on the extent and nature of the breach.

If the breach occurs or is discovered outside normal working hours, the investigation and notification of relevant officers should begin as soon as is practicable.

Records must be kept of all actions taken. The ILO is responsible for collating all records.

2.2. Assessment of an Ongoing Breach

The nature of the breach will determine what steps are necessary in addition to immediate containment. This will be done by an assessment of the risks associated with the breach. This risk assessment will be undertaken by the ILO.

The most important aspect is an assessment of potential adverse consequences for the individuals, how serious or substantial these are and how likely they are to happen. This will be based on:

- What type of data is involved?
- How sensitive is the data?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- Regardless of what has happened to the data, what could the data tell a third party about the individual?
- How many individuals' personal data are affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals and/or to the Council?

2.3. Notification of the Breach

The ILO shall determine who will be notified, the information the notification will contain and how they will be notified. In determining the extent of the notification the following should be considered (this is not an exhaustive list and each breach must be assessed on its own circumstances):

- Which individuals and/or groups, including Council staff, need to be notified?
- What are the dangers of 'over notifying'?
- Any contractual or operational requirements?
- Which regulatory bodies require notification?
- Can notification help the Council to meet its security obligations with regard to the seventh data protection principle?
- Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the notification to mitigate risks to themselves?
- How many people are affected?
- How serious are the consequences?
- How the notification can be made appropriate for particular groups of individuals.

2.3.1 Determining Serious Breaches

The presumption is that all breaches are 'serious' breaches unless the facts of the breach indicate otherwise.

The ILO must determine if the breach is a serious breach that needs to be notified to the Information Commissioner's Office (ICO). Where necessary the ILO should work with the Regulation Team to determine if the breach is 'serious' for the purposes of notifying the ICO.

In order to establish the seriousness of a breach the following must be considered:

- The potential harm to the data subject as a result of the breach, including any distress the data subject may suffer as a result of the breach, which is dependent on the volume and the sensitivity of the data involved.
- The volume of the data involved - this must be determined by the facts and extent of the breach.

- The sensitivity of the data involved - where the data is classed as sensitive personal data as defined by section 2 of the Data Protection Act 1998 and the release of that data can lead to the data subject suffering substantial harm.

Serious breaches should be notified to the ICO and the notification should include details of:

- The type of information and number of records
- The circumstances of the loss / release / corruption
- Actions taken to minimise / mitigate effect on individuals involved including whether they have been informed
- Details of how the breach is being investigated
- Whether any other regulatory body has been informed and their response
- Remedial action taken to prevent future occurrence
- Any other information that may assist the ICO in making an assessment

2.4. Evaluation and Response

Once the breach has been dealt with the ILO should evaluate and report to the Senior Information Risk Owner and Head of Governance on the effectiveness of the Council's response to the breach.

Where the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if the Council's response to the breach was hampered by inadequate policies or a lack of a clear allocation of responsibility then any response must review and update these policies and lines responsibility accordingly.

The evaluation must consider, although not limited to:

- Ensuring those who need to be aware know what personal data is held and where and how it is stored.
- Establishing where the biggest risks lie.
- Ensuring that where data is shared, either internally to the Council or externally, the method of transmission is secure and that only relevant data is shared or disclosed.
- Identifying weak points in existing security measures.
- Monitoring staff awareness of security issues and looking to fill any gaps through training or tailored advice

2.5 Employment Considerations

This policy should be read in conjunction with the ICT Policy and the Employee Code of Conduct:
http://insite/sites/intranet/InformationLibrary/Files/ICT%20Policy.pdf
http://insite/sites/intranet/InformationLibrary/Files/Code%20of%20Conduct%20for%20Employees.pdf

Where a breach of this policy has occurred it may result in action being taken in accordance with the council's disciplinary policy.

3.1. Monitoring and Review

This policy shall be reviewed every 12 months after implementation.

3.2. Implementation

This policy was implemented on XXXX

4.1. Contacts

Helen Edwards	Solicitor to the Council and Senior Information Risk

	Owner 01733 452539
Diane Baker	Head of Governance 01733 452559
Steve Crabtree	Chief Internal Auditor 01733 384577
Louise Tyers	Compliance Manager (Regulation) 01733 452284
Alana Diffey	Information Specialist 01733 452276

Appendix 1

Data Protection Breach - Record of Actions Taken - Confidential

Date of breach:	
Description of the data involved:	
Summary of incident:	
Staff/Team involved:	
Investigation Lead Officer: **(name & job title)**	
Outcome of investigation:	
Date resolved:	

Who to inform

✓		**Date completed**
	Manager of officer that discovered the breach	
	Head of Governance (who will appoint an Investigation Lead Officer)	
	Senior Information Risk Owner (Solicitor to the Council)	
	Head of Communications	
	Chief Internal Auditor	
	Director(s) (where necessary)	
	All relevant staff	
	Police (where necessary)	
	Data Subject(s) (where necessary)	
	Regulatory Body (where necessary)	
	Information Commissioner's Office ('Serious' breaches only)	

<u>Stolen data or equipment</u>

✓		**Date completed**
	Inform the police	
	Get a crime reference number Ref. no:	
	Inform ICT Service Desk	
	Inform PCC Insurance	

The Investigation

The investigation should cover the following, and records must be kept of any searches and actions undertaken. All of this information must be retained as evidence of the investigation.

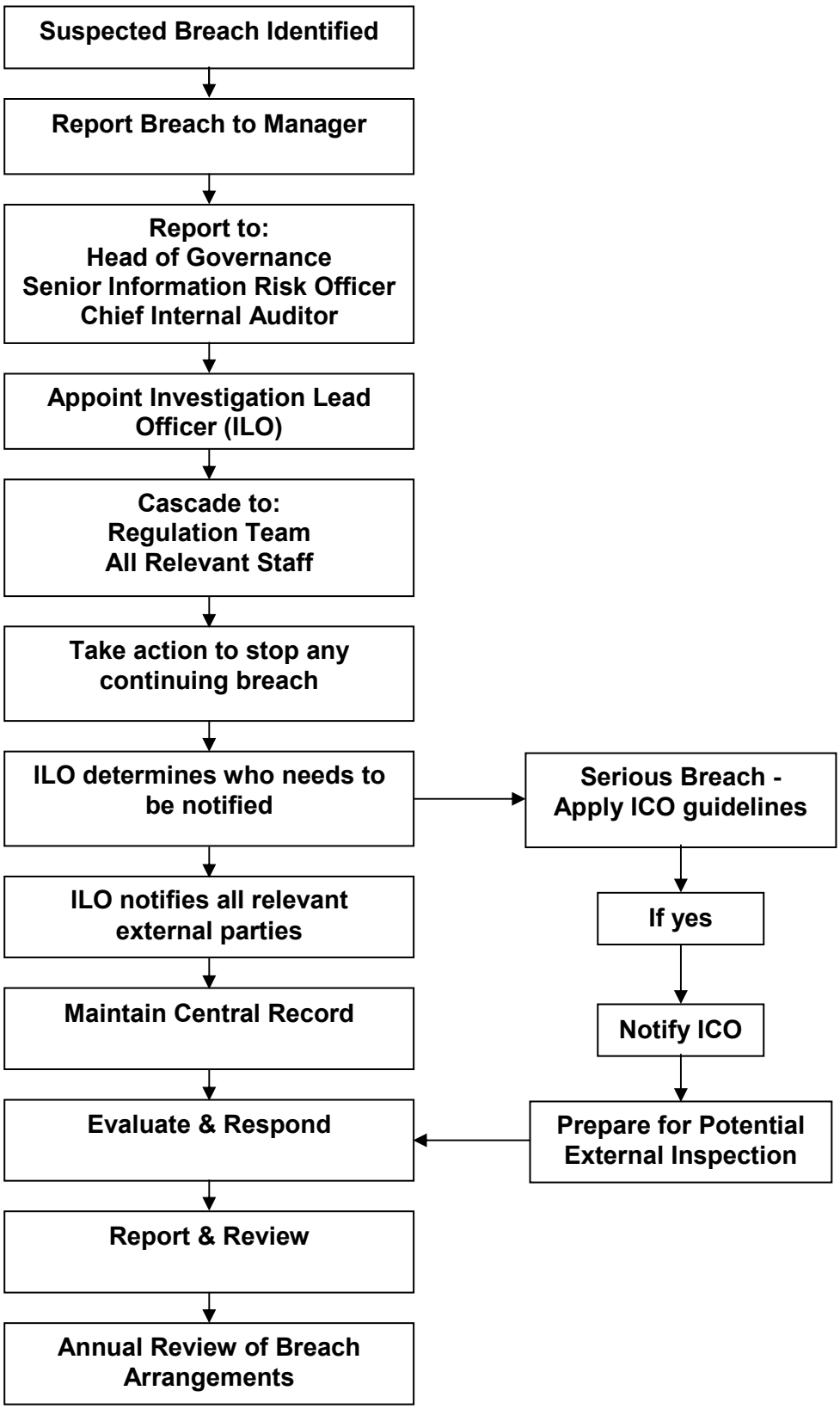
✓		**Date completed**
	Undertake extensive searches for any physical loss	
	If the data has been lost, and is in paper form only, consider reporting this to the police	
	Assess whether the data subject(s) should be informed of the breach	
	Assess whether the Information Commissioner's Office (ICO) should be informed of the breach	
	Report on the reason(s) for the data breach. If this was due to a lack of operational policy or procedure, this should form part of the report into the breach and be fed back to the relevant senior management team and the Regulation Team	

If the decision is made to inform the data subject

✓		**Date completed**
	All details necessary to be able to take mitigating actions	
	Include their right to complain to the Council and the ICO	
	Provide details of what the Council has already done to respond to the risks posed by the breach	
	Provide details of the Investigation Lead Officer if they need to contact the Council for further information, or if they have any questions regarding the investigation	

Appendix 2

Data Protection Breach Process Flow Chart



This page is intentionally left blank