



Great Yarmouth Borough Council Data Handling & Security Breaches

Author	Geoff Jones
Date	17 March 2009
Version	3.0
Last Review Date	1 March 2011
Review Changes	Section 2.4 modified for transporting hard copy information
Document Status	Final

1.0 INTRODUCTION	3
1.1 POLICY RATIONALE.....	3
1.2 SCOPE	3
1.3 PRINCIPLES	4
2.0 DATA HANDLING & SECURITY BREACHES.	4
3.0 IMPLEMENTATION AND COMPLIANCE.....	16
3.1 IMPLEMENTATION.....	16
3.2 COMPLIANCE.....	16
4.0 EQUALITY IMPACT ASSESSMENT	16
5.0 HEALTH AND SAFETY	16
6.0 REFERENCE DOCUMENTS.....	17
7.0 DISTRIBUTION	17
8.0 REVIEW.....	17

1.0 INTRODUCTION

This policy forms part of the suite of policies dealing with data security.

The use of IT networks by staff from Great Yarmouth Borough Council is an essential business requirement to keep in step with the demands for the retrieving, collating and communicating of information, in a fast, economic and secure manner.

The aim of this Data Handling & Security Breach policy is reduce the risk to the integrity and reputation of Great Yarmouth Borough Council, while maximising the use of these important business tools.

Security is a holistic issue; it's not the network we need to protect, it's the information inside that network and that means guarding against data leaks as well as network intrusions.

Email is where a significant amount of the knowledge, expertise and relationships within businesses is stored, although the combination of storage demands and unmanaged archives often make it as much of a problem as a resource. Email has become a critical business tool, but it is also the easiest way for information to escape from the confines of a business.

1.1 POLICY RATIONALE

At the time of the writing of this Data Handling & Security Breach policy in 2009, the council was aiming to meet the requirements to obtain and use a government connect secure circuit.

In 2009, the Council was of the view that there was a need to ensure that an agreed standardised approach was being taken to Data Handling & Security Breaches, in order to protect Council assets, and to ensure compliance with audit requirements.

This policy seeks to establish a standard set of conditions, and a framework for Data Handling & Security Breaches within the Council.

1.2 SCOPE

This Policy will apply to all Council employees who are required to view or receive data to assist them in the performance of their duties.

1.3 PRINCIPLES

The Policy is designed to ensure that there are clear internal arrangements for the effective management of Data Handling & Security Breaches.

2.0 DATA HANDLING & SECURITY BREACHES.

All areas of the council handle data in various forms, hard copy, electronic, verbal this data must be classified before it is used or stored. Information received by the Government Connect route can potentially be classified up to confidential level.

Regardless of its classification care must be taken when handling data, if data is lost, seen by unauthorised persons or sent outside of a secure domain then actions must be taken to minimise the result of the breach.

The classifications used are:

- Not Protectively Marked
- Restricted
- Confidential
- Secret
- Top Secret

Would accidental or deliberate compromise of this data be likely to?

Restricted	Confidential	Secret	Top Secret
Cause substantial distress to individuals	Prejudice individual security or liberty	N/A	N/A
Make it more difficult to maintain operational effectiveness	Work substantially against national finances or economic and commercial interests		
Prejudice the investigation or facilitate the commission of a crime	Substantially undermine the financial viability of major organisations or the council		
Impede the effective development or operation of policy	Impede the investigation or facilitate the commission of a serious crime		
Breach proper undertakings to maintain the confidence of material provided by third parties	Seriously impede the government policies		
Breach statutory restrictions on disclosure of materials	Shut down or otherwise substantially disrupt significant operations		
Disadvantage the council in commercial or policy negotiations with others			
Undermine the proper management of			

the public sector and its operations			
--------------------------------------	--	--	--

2.1 POLICY ENFORCEMENT

This policy and supporting procedures cover a number of distinct areas which include:

- Training and awareness
- Creation and marking of proactively marked data
- Storage and handling
- Security and access
- Archiving and weeding
- Disposal
- Monitoring and audit of procedures

All data, paper, electronic, will be protectively marked according to pre-defined classifications. This can be by a stamp or handwritten signed note on the top and bottom of each page of the document.

The policy should not be viewed as a barrier to interfere with council business but as a contribution to secure effective business.

2.2 CREATION AND MARKING OF MATERIAL

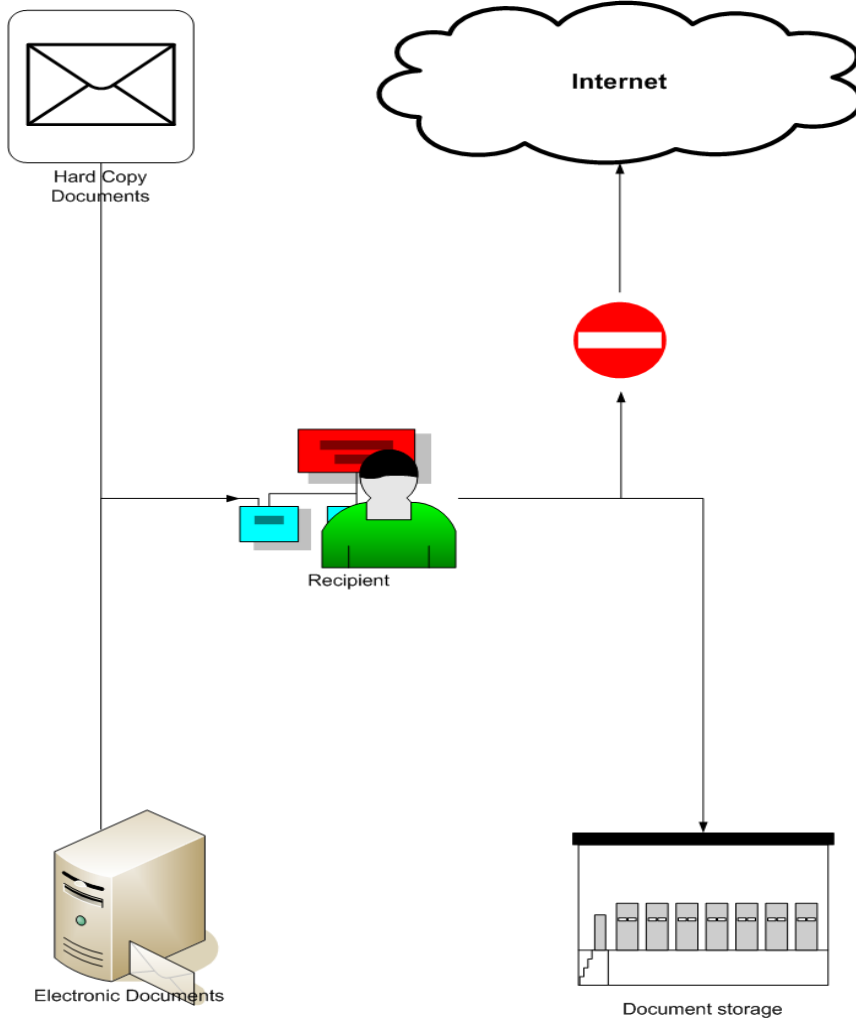
On creation or receipt of a document or data it will be classified. It is the responsibility of the author of a document or data to risk assess it in order to ascertain the appropriate level of classification.

The recipient of documents or data originated elsewhere must risk assess and protectively mark these.

Routine marking of 'legacy documents' will not be carried out until they are required for use at which point and before they are used partly or in full they will be risk assessed and protectively marked.

All documents will be classified prior to use. It is the recipient's responsibility to mark the document if it has not already been done.

No documents containing personal, restricted or classified information will be sent via the internet unless it is on the encrypted circuit.



2.3 CLASSIFICATION LEVELS

Definitive levels to classify documents or data cannot be given but the following guidance must be taken into account when defining the classification.

Impact if the data is lost or stolen and misused	Classification	Examples
<p>Inconvenience to customers</p> <p>Minor damage to the departments standing or reputation</p>	<p>Not Protectively Marked</p>	<p>Personal data such as name and address for which we have a duty of care</p> <p>Combinations of data that is in the public domain or could be placed in the public domain without causing the customer economic harm</p>
<p>Substantial inconvenience or distress</p> <p>Significant financial impact to the customer</p> <p>Substantial damage to the departments reputation or standing</p> <p>Prejudice the investigation of or facilitate the commission of crime</p> <p>Could have wider implications within the local authority</p>	<p>Restricted</p>	<p>A complete customer record including personal financial and or banking details</p> <p>Volumes of not protectively marked data about a reasonably large number (hundreds) of customers.</p> <p>A small number of high profile or vulnerable customers</p>
<p>Prejudice the safety or liberty of an individual</p> <p>Impede the investigation of facilitate the commission of a serious crime</p>	<p>Confidential</p>	<p>A large number of complete customer records</p> <p>A set of data relating to many customers which in combination could result</p>

<p>Could have wider implications with in the local authority or wider area</p>		<p>in identity theft</p>
--	--	--------------------------

Examples

A council tax letter containing name, address and amount owed would not be protectively marked

A batch of 200 letters containing the same information would be marked as restricted whilst in the batch

Whereas the new years bills, 40,000+, would be marked as confidential whilst in the batch.

However, if the letter contained the name, address and bank account details then this would be marked as restricted.

2.4 HANDLING INFORMATION

As a general rule information should not be removed from or accessed outside of the council's environment.

If it is necessary for this to occur then thought must be given taking into account the marking on the information.

If it is not protectively marked then the standard duty of care applies

If it is marked as restricted or confidential then it must be encrypted with the password kept separately. This type of file must not be emailed over the internet but only via the secure network.

If the information is in hardcopy form and is marked restricted or confidential it must be transported in a locked case or sent by other approved secure methods such as the DX system.

If a secure method is being used the documents must be in a sealed envelope marked with the recipients name and restricted or confidential. This must then be placed in another sealed envelope marked with the recipients address but this must not be marked restricted or confidential.

Information sent this way must be delivered within 24 hours so for example if you use the DX system do not send on a Friday as it will not be delivered until Monday.

Any information sent to a third party must be logged centrally and a message must be sent to the recipient informing them the information is on its way.

Destruction of the data by the recipient once it is no longer required must also be assured.

Copying of information should be avoided; apart from raising questions regarding its accuracy keeping an audit trail becomes difficult.

Any information marked higher than Not Protectively Marked (Impact Level 2) must be booked out and signed back by the recipient; this audit trail must be kept for the life of the information plus 1 year.

A clear desk policy must be kept for any information restricted (Impact Level 3) or above, this means information must be locked away or returned to the central store each night.

Any information marked confidential (Impact Level 4) must also be locked away when leaving the desk at anytime.

2.5 STORAGE AND ACCESS

Thought must be given to the storage of the information. Most will accept and store information in electronic areas designated.

What about the printed copy?

Do you need to print a copy of the information?

Where are you storing this copy?

Again some guidance can be given:

- You have a general duty of care for all printed information, don't leave it around.
- Any information marked restricted or above must be locked away when not in use, this especially includes lunch and when leaving for the day.

Who needs to see the information?

Very simply any information should be used and viewed on a need to know basis, it may well be interesting that a well known local figure has an outstanding debt but does everyone need to know that.

2.6 ARCHIVING AND WEEDING

All information must have a life, after which it must be destroyed.

The life designated must be reasonable for the information involved; you cannot say you will keep this information forever just to avoid having to delete it.

Any information archived must be kept in a location appropriate to its designation access to the location must be commensurate and monitored dependent on the information stored there.

2.7 DISPOSAL

2.7.1 HARDCOPY

General Hardcopy data containing information where a person can be identified must be disposed of in confidential waste; this is our duty of care when handling information.

Thought needs to be given when disposing of restricted information, disposal in confidential waste may be acceptable but consideration to separation of pages or shredding should be given.

When disposing of confidential waste this must always be shredded.

2.7.2 ELECTRONIC

General electronic information can be deleted using the standard Microsoft delete function.

Restricted and confidential information must be electronically shredded when deleted.

Remember when deleting data to check that any backups are also removed.

2.8 MONITORING AND AUDIT OF PROCEDURES

To ensure compliance the file containing details of the restricted and confidential information will be audited yearly, during the year random checks will also take place to ensure information is being booked in and out correctly.

If documents are received that has been accessed or generated internally and has not been correctly marked then the recipient must raise an incident. These incidents will be investigated appropriate actions and reminders made.

2.9 SECURITY BREACH PROCESS

If a breach is suspected the first step is to inform the support desk, they will raise an incident that will alert the data security manager of the potential breach.

The security manager will with the nominated departmental officer identify the sensitivity of the data, whether it is internal or client data and what level of protection was in place.

A crises management team will be formed its composition will vary depending on the severity of the leak but will as a minimum consist of the data security manager, the nominated officer from the affected section and a member of the sections management team. If the leak is more serious then members of the executive board, HR and communications must be included.

Establish whether the lost data can be accessed or used without specialist knowledge of software.

With knowledge of the above assess the impact on the data subjects and the council.

Determine whether the loss was opportunistic, targeted or due to a lapse in security

Determine if legal tests for liability are proven

Identify the location of the loss and whether recovery is possible

List the data subjects affected and their contact details

Draft communications for public and private notifications to the data subjects and the information commissioner's office.

Reference the loss against internal policies to identify any weakness

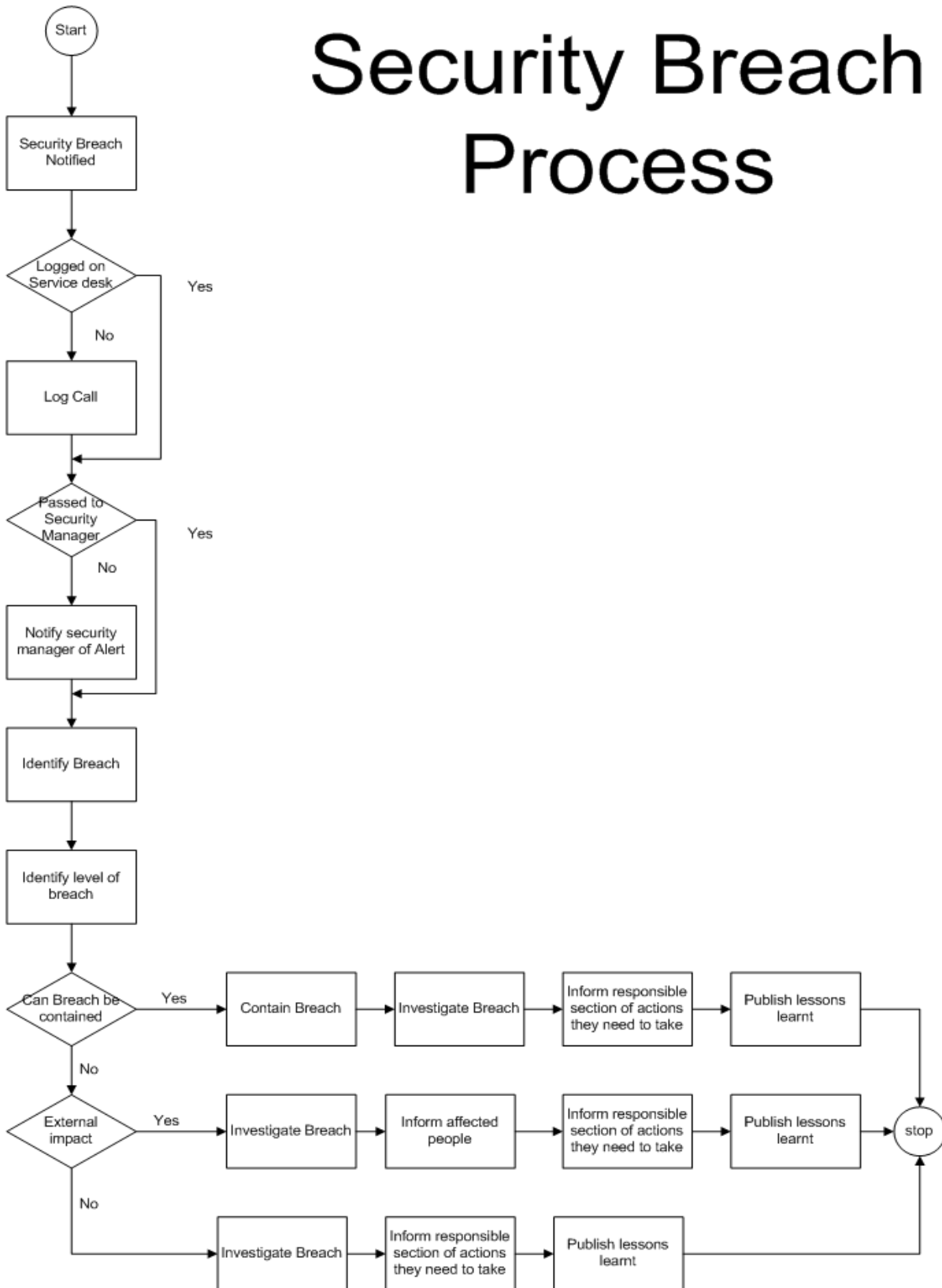
At this point the material facts should be known all parties will have been identified and informed and immediate remedial actions undertaken. Consideration can now be given to the wider issues.

If necessary consultation with specialist legal advisers

A review of policies and processes to ensure a second loss is not suffered and that current measures are fit for purpose.

Establish if policies and procedures have been followed.

Security Breach Process



3.0 IMPLEMENTATION AND COMPLIANCE

3.1 IMPLEMENTATION

This policy will initially be implemented through the Chief Executive and Corporate Directors of the Council.

A memo will be sent to all HOD's and SUM's to make them aware of the policy.

It is the responsibility of managers to ensure that new staff receive information about this Policy, and should be part of any local induction where appropriate. Human Resources will add the Policy to its list of policy issues provided to any new starters. Managers must also ensure that any changes to this policy are effectively communicated within their areas of responsibility.

3.2 COMPLIANCE

Managers are responsible for ensuring that staff are aware of the location of this policy. In addition, Managers are responsible for keeping staff up to date about any changes within the policy.

All staff that receive restricted information are obliged to adhere to this Policy.

4.0 EQUALITY IMPACT ASSESSMENT

An equality impact assessment has been undertaken for the suite of policies relating to data security.

The result of this assessment shows low relevance in relation to specific equality issues and factors.

The full assessment can be found at:

<I:\Equality & Diversity\EIA\Equality Impact Assessments\Gov Connect\data security EIA.doc>

5.0 HEALTH AND SAFETY

There are no health and safety implications with this policy.

6.0 REFERENCE DOCUMENTS

This Policy should be read in conjunction with the following legislation, regulations and Council policies:

- COCO security checks
- System Access and Passwords
- Internet Security
- Email Usage
- IT Security
- Using Removable Media
- Contractors / Suppliers connecting to the GYBC network
- Taking GYBC computer equipment abroad

7.0 DISTRIBUTION

This Policy will be available for all the Council's designated locations. Copies will also be available from the 'I' drive and on the Council's Intranet.

8.0 REVIEW

This Policy will be reviewed on an annual basis with the next review date being April 2012.