DATA LABEL: Official

AUTHOR: Roberto Riaviz
TITLE: Technical Strategy Manager
DOCUMENT TITLE: Information Handling Procedure

Review/Approval History

<table>
<thead>
<tr>
<th>Date</th>
<th>Name</th>
<th>Position</th>
<th>Version Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>20/08/2009</td>
<td>Information Management Working Group</td>
<td>N/A</td>
<td>1.6</td>
</tr>
<tr>
<td>05/08/2009</td>
<td>IT Services Management Team</td>
<td>N/A</td>
<td>1.6</td>
</tr>
<tr>
<td>06/04/2010</td>
<td>ICT Programme Board</td>
<td>N/A</td>
<td>1.6</td>
</tr>
<tr>
<td>28/04/2010</td>
<td>Corporate Management Team</td>
<td>N/A</td>
<td>1.6</td>
</tr>
<tr>
<td>07/07/2015</td>
<td>Information Management Working Group</td>
<td>N/A</td>
<td>2.1</td>
</tr>
<tr>
<td>14/03/2016</td>
<td>Information Management Working Group</td>
<td>N/A</td>
<td>2.1</td>
</tr>
</tbody>
</table>

Change Record Table

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Version</th>
<th>Status</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/01/2009</td>
<td>Roberto Riaviz</td>
<td>1.0</td>
<td>Draft</td>
<td>Initial draft</td>
</tr>
<tr>
<td>06/04/2010</td>
<td>Roberto Riaviz</td>
<td>1.6</td>
<td>Final</td>
<td>Updated re comments received</td>
</tr>
<tr>
<td>28/04/2010</td>
<td>Roberto Riaviz</td>
<td>2.0</td>
<td>Final</td>
<td>Approved Final Copy</td>
</tr>
<tr>
<td>07/07/2015</td>
<td>Roberto Riaviz</td>
<td>2.1</td>
<td>Final</td>
<td>Updated links and data classifications</td>
</tr>
</tbody>
</table>

Status Description:

Draft - These are documents for review and liable to significant change.

Final - The document is complete and is not expected to change significantly. All changes will be listed in the change record table.
West Lothian Council

Information Handling Procedure

Contents

1.0 Background .................................................................................................................................................. 3
2.0 Legal Requirement ........................................................................................................................................ 4
3.0 Identifying Personal Information ................................................................................................................... 4
  3.1 Registration of Personal Information ........................................................................................................... 4
  3.2 Classification of Information ....................................................................................................................... 4
  3.3 National Classifications .............................................................................................................................. 4
  3.4 OFFICIAL SENSITIVE classification (for Personal Information) .............................................................. 5
  3.5 West Lothian Council Information Classification Scheme ....................................................................... 5
4.0 People ............................................................................................................................................................ 7
  4.1 Staff Awareness ........................................................................................................................................... 7
  4.2 General Staff Guidance ............................................................................................................................. 7
  4.3 Security Incident Reporting ....................................................................................................................... 8
  4.4 System Owners .......................................................................................................................................... 8
  4.5 User Access Rights ................................................................................................................................... 8
  4.6 Staff Induction and Exit procedures ........................................................................................................ 8
5.0 Places .......................................................................................................................................................... 9
  5.1 Security of buildings and premises ............................................................................................................ 9
  5.2 Secure Disposal of Information ................................................................................................................ 9
  5.3 Paper Records .......................................................................................................................................... 9
  5.4 Electronic Records .................................................................................................................................. 10
  5.5 Public Offices ......................................................................................................................................... 10
6.0 Processes ...................................................................................................................................................... 10
  6.1 Data/Information Labelling ....................................................................................................................... 10
  6.2 Systems Access to Information ................................................................................................................ 11
  6.3 Mobile Devices/Removable Media (Laptops etc.) .................................................................................... 11
  6.4 Email ....................................................................................................................................................... 12
  6.5 Transfer/Sharing of Information (information in transit) ..................................................................... 12
  6.6 Storage of data/information (information at rest) ................................................................................... 13
  6.7 Faxing, Printing and Copying .................................................................................................................. 13
  6.8 Testing .................................................................................................................................................... 13
  6.9 Privacy Impact Assessments .................................................................................................................... 13
  6.10 Third Party Access .................................................................................................................................. 14
  6.11 New ICT Systems and Information Security Tools ............................................................................... 14
  6.12 Clear Screen Policy ................................................................................................................................ 14
  6.13 Risk Management .................................................................................................................................. 14
  6.14 Summary of Information Handling Requirements by Classification .................................................... 15

Data Label: Official
West Lothian Council

Information Handling Procedure

1.0 Background

Within West Lothian Council, modern service delivery is becoming increasingly dependent on the effective use and exchange of information. Information is routinely exchanged with citizens, within and between service areas and with other public and private service partners.

By the very nature of council services, personal data and information (relating to individuals) is regularly collected, processed and stored on behalf of the public. In order to maintain service credibility, it is crucial that the public have confidence that any data provided by or about them is handled appropriately. This means that personal information is handled with sensitivity and confidentiality whilst at the same time, ensuring that appropriate measures are in place to reduce risks of loss or misuse.

Throughout the UK, security incidents involving misuse and loss of information are keenly reported in the media. Recent losses of personal data such as that from Her Majesty’s Revenue and Customs now require that all public bodies act to bolster public trust and confidence in the way personal information is handled and protected.

There is a statutory responsibility under the Data Protection Act (1998) that the council handles all personal information with appropriate levels of protection. From 6 April 2010, the Information Commissioner’s Office (The UK governing body on the Data Protection Act) has new powers to issue monetary penalties up to £500,000 for serious breaches of the Data Protection Act.

Where council services follow the procedures set out within this document, they will significantly reduce the risk of information security incidents and issues. In doing so, they also reduce the potential impact caused by damage or loss of information. The impact of such incidents includes: personal distress; risk to members of the public; damage to reputation; legal action; loss of public confidence; disruption to services and recovery costs.

It should be noted that this procedure indicates a minimum standard to be followed by all services. Where information sets within the council are considered to be of higher risk, more stringent security arrangements may be deemed necessary. A robust risk analysis must be conducted to ensure the operation of appropriate security measures in all service areas.

The procedures form part of an information assurance document framework that includes an Information Security Policy as well as corporate and service based guidelines and procedures.
2.0 Legal Requirement

The council has a legal requirement to protect personal information it manages. The seventh principle of the Data Protection Act 1988 requires that the council takes: “Appropriate technical and organisational measures ... against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”.

The council’s Data Protection Policy can be viewed on the Intranet or by following this link: WLC Data Protection.

3.0 Identifying Personal Information

3.1 Registration of Personal Information

Most systems within the council will contain some personal information. It is necessary that all systems that contain personal information, including paper based systems, are recorded in a central register. This should be done via the Information Security Officer: InfoSec@westlothian.gov.uk.

All systems containing personal information will be entered in the council’s risk register. All associated risks will be recorded, monitored and managed as per the council’s Risk Management Procedure.

3.2 Classification of Information

Classifying information means that appropriate levels of safeguards can be applied at each security level. It would be difficult, cumbersome and expensive to apply high level security controls to all information.

The UK Government uses a ‘Protective Marking Scheme’ that classifies information at a national security level. This includes levels such as TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED (in descending order of sensitivity).

3.3 National Classifications

As a rule of thumb, all Government Classified information (marked Top Secret, Secret and Confidential) is ‘for your eyes only’ and should not be viewed by anyone else. Hard copy documents must be locked away.

Access to RESTRICTED information is normally subject to strict controls e.g. VISOR, Government Secure Extranet (GSX), and Government Secure Intranet (GSI). Procedures and protocols are already in place (at a system level) and must always be observed.

Access to systems are always strictly controlled and managed by specific government departments. Care should be taken not to access download or store such information without prior permission. Data and information labelled with these markings MUST NOT be stored on the council EDRM system or network drives. For further information and advice on how to handle this small subset of information, please contact the council’s records manager.

The vast majority of information within West Lothian Council will not be subject to the national security markings.
3.4 OFFICIAL SENSITIVE classification (for Personal Information)

From 2008, a new (sub-national security marking) classification has been added by UK Government. The new classification, called “Official – Sensitive” will include personal and sensitive information that is routinely managed within councils and between government departments. (This includes the non-restricted information on the Government Secure Extranet (GSX), and Government Secure Intranet (GSI)).

The Government has defined personal data as that whose release or loss could cause harm or distress to individuals. As a minimum, it defines this as any information that links an identifiable living person with information about them whose release would put them in significant risk of harm or distress. To illustrate this, any one piece of personal information from section A (below) in conjunction with any piece of information from section B (below) would warrant a security marking of ‘Protect’.

A. This is any piece of information that could be used along with publicly accessible information to identify a person e.g. name, address (home, business or both), postcode, email address, telephone number, driving licence number and/or date of birth.

B. Information whose release is likely to cause harm or distress includes sensitive personal data such as DNA or fingerprints/bank, financial or credit card details/mother’s maiden name/National Insurance Number/Tax, benefits or pension records/health records/employment record/school attendance or records/material relating to social services including child protection and housing.

In Addition: Section 2 of the Data Protection Act defines personal data as relating to racial or ethnic origin; sexuality; membership of a trade union; political opinions, religious beliefs or similar nature; physical or mental health details; commission or alleged commission of any offence; proceedings for any offences alleged or committed.

As well as the above, included in this ‘Official - Sensitive’ category is any source of information about 1000 or more identifiable individuals, other than information sourced from the public domain. This could be a database with 1000 or more entries containing facts mentioned in A (above), or an electronic folder or drive containing 1000 or more records about individuals. Again, this is a minimum standard. Information on smaller numbers of individuals may warrant protection because of the nature of the individuals, nature or source of the information, or extent of the information.

3.5 West Lothian Council Information Classification Scheme

In order to encompass (and simplify) the above, the following chart identifies classification scheme that applies to all information within West Lothian Council:

(The remainder of this document describes the minimum requirements to secure personal information within West Lothian Council.)
# West Lothian Council Information Classifications:

<table>
<thead>
<tr>
<th>Information Class</th>
<th>LEVEL DESCRIPTION</th>
<th>Subject to F.O.I.</th>
<th>Subject to DATA PROTECTION</th>
<th>WHO CAN ACCESS IT</th>
<th>EXAMPLE GROUPS</th>
</tr>
</thead>
</table>
| 1 Classified ‘For your eyes only’ | This is the top level of information security and is applied to information where the council has an obligation and/or responsibility to maintain the confidentiality of information. This level includes Government Classified, ‘Security Marked’ Sensitive Personal Information, and Politically Sensitive information. | The detail of such information is normally exempt from FOI | Any personal information will be subject to DP | • Named Individuals (only)  
• Pre-identified groups of ‘Privileged’ Users  
• Further restrictions on viewing/copying/ printing may apply | Case Officers, Heads of Service, CMT, Directors etc. |
| 2 Official – Sensitive ‘Accessed for business purposes only’ | This information is normally restricted only to those staff who need access in order to carry out their duties. Such information is not made publicly available because of its sensitive nature e.g.  
• Personal information  
• Personnel information  
Commercial in confidence etc. | The detail of such information may be exempt from FOI | All personal information will be subject to DP | • Named Individuals  
• Pre-identified groups of ‘Privileged’ Users  
• Requires an awareness of Data Handling Guidelines/Procedures | Management Teams  
Project Teams, Operational Teams, Service Areas etc. |
| 3 Official – Internal ‘Available to all council staff’ | This includes all information ‘published’ internally i.e. made available to all staff such as general Council and ‘Service- Specific’ information held in shared files and on the Intranet, e.g. Phone Book, Policies, Procedures, Performance statistics etc. | Yes | No | • All WLC | All WLC Staff Partners Suppliers |
| 4 Public ‘Available to all council staff and the general public’ | Can be published to the internet etc.  
No restrictions on viewing (subject to the publishing process required of publication scheme)  
Declared records of public interest | Yes | No | Anyone | |
| 5 Not Protectively Marked | Personal Information, Non-Business information or transitory in nature. | No | No | Anyone | Individuals |
4.0 People

“Each service area should seek to develop a culture that properly values, protects and uses information for the public good. Information is a key business asset and its proper use is not simply an IT issue. There should be clear lines of accountability throughout the service together with a programme of staff awareness raising, starting at induction, but continually updated, which clearly sets out the expectations of staff”.

Local Government Data Handling Guidelines – SocITM (in association with the Local Government Association and Solace)
November 2008

4.1 Staff Awareness

All staff should be aware that there is a new council policy on Information Security (August 2008). The policy can be accessed via ‘My Toolkit’ (HR Employment Policies Section) or by following this link: Information Security Policy.

There is an ‘online’ video on the council’s intranet that explains the fundamentals of information security. All managers must ensure that all staff (with a priority of those who handle personal information) have viewed the video (and completed the online tests – each member of staff must save/print a certificate as proof of completion).

Security Awareness Video.

A DVD disk can be supplied to staff that do not have network access to the above intranet pages. For details, contact the IT Service Desk: itservicedesk@westlothian.gov.uk.

Other material will continue to be produced to support staff awareness such as Intranet pages, email updates, posters, brochures, leaflets etc.

For services with high-risk information handling issues, specific promotional material can be produced. A request should be made to the Information Security Officer: InfoSec@westlothian.gov.uk.

In order to monitor the effectiveness of Staff awareness programmes, Internal Audit will conduct ‘spot checks’ and sample audits on an annual and ongoing basis.

4.2 General Staff Guidance

All staff are encouraged to use common sense judgment in protecting the council’s Protected information (treating it as they would their own bank details). If anyone is uncertain of the sensitivity of a particular piece of information, they should first contact their line manager.
4.3 Security Incident Reporting

All staff are encouraged to report any known or suspected security incidents immediately. This includes any unfamiliar or suspect activity within offices or within systems. Such incidents include but are not limited to computer viruses, system outages or failures, lost documents/files, lost or stolen data/information/devices.

Staff should feel comfortable in reporting any losses, however inadvertent. The sooner such incidents are reported, the sooner procedures can be activated to contain, reduce or minimise the impact(s) of such losses.

All information security incidents **must** be reported to the IT Service Desk in the first instance: Email: itservicedesk@westlothian.gov.uk, Tel: 01506 282828.

4.4 System Owners

Each information system (manual or computer based) must be assigned an ‘owner’. This is a ‘business’ owner who acts as an asset manager for the information contained within that system. Their role is to understand what information is held, how it is used and transferred, and who has access to it and why, in order for business to be transacted with acceptable level of risk. The ‘owners’ of information must have sufficient delegated authority to make decisions based on risk management, security incidents, budget approvals etc.

4.5 User Access Rights

System Owners and/or Systems Administrators must ensure that users ‘Access’ rights (to facilities and systems) are regularly reviewed and amended as required. Users are those staff, contractors and suppliers who access and process information (especially personal and sensitive information) for and on behalf of the council. By default, staff should have the minimum access to systems containing personal protected information. Where greater access is necessary, it should be to the smallest possible subset of staff and records. Appropriate levels of awareness and training **must** be provided to staff that are entrusted to process personal protected information.

4.6 Staff Induction and Exit procedures

All staff starting work with the council must be notified of their responsibilities regarding personal protected information. This includes permanent, part time, job share, temporary staff, contract staff, suppliers, agency staff etc.

There must be a single user account (for network, email and applications) set up for each user who has access to West Lothian Council systems. ‘Generic’ accounts e.g. ‘IT Services’ **must not** be used for any systems that contain personal protected information.

On leaving the organisation, all staff accounts **must** be suspended immediately. In some situations, where highly sensitive information is at risk, it may be necessary suspended user accounts before people leave the organisation. All unused user accounts will be suspended after 30 days of inactivity. All suspended user accounts will be deleted after 30 Days (unless informed otherwise).
All managers **must** ensure that IT Services are notified to remove network and email accounts at the appropriate time.

### 5.0 Places

All services should ensure the security of information through the physical security of their buildings, premises and systems. There should be regular assessments of information related risks. All risks should be logged on the council’s Risk Register.

#### 5.1 Security of buildings and premises

In buildings where personal ‘Protected’ information is managed:

All staff **must** be provided with council ID cards. Managers must ensure that badges are worn at all times. Anyone who is not wearing a badge should be challenged. Lost or stolen badges should be reported immediately to: facilities@westlothian.gov.uk.

All visitors to buildings **must** be recorded and wherever feasible, ensure that they are accompanied whilst on the premises.

A clear desk/clear screen policy **must** be implemented to reduce the risk of unauthorised access, loss or damage to information.

Where personal information is held on paper, it **must** be locked away when not in use.

All laptops and removable media **must** be safely locked away when not in use.

Care **must** be taken to ensure that conversations regarding ‘Protected’ information are not conducted in environments where such dialogue can be overheard.

#### 5.2 Secure Disposal of Information

As it reaches the end of its useful life all personal information/data **MUST** be destroyed securely. For general advice information disposal, please contact the council’s records manager.

#### 5.3 Paper Records

All personal information **must** be securely destroyed (when no longer required). The council’s disposal procedure should be followed. Link to Guidelines: Information Destruction Guidelines

‘Protected’ documents are to be destroyed by shredding on council approved shredders.*

Particularly sensitive information or information with higher security classifications **must** be collected for secure destruction. Confidential waste must be kept in a secure location at all times.

For further information and advice on document destruction, please contact the council’s records manager.

* Shredder standards are currently being developed by the Records Manager in conjunction with Facilities Management and will be rolled out across the council.
5.4 Electronic Records

Electronic information media must be identified to IT Services who will arrange destruction appropriate to council standards. Media can include CDs, DVDs, PCs, Laptops, Servers, USB Sticks, Flash Drives, USB Pens, Printers etc.

Where any media is being re-used (within or outwith the council) it must be cleared of data. The cleaning process must be to council standards.

To arrange equipment destruction or data cleansing, contact the IT Service Desk: itservicedesk@westlothian.gov.uk. For further advice on secure destruction, contact the Information Security Officer: InfoSec@westlothian.gov.uk.

5.5 Public Offices

Public Offices, counters and reception areas should be free from the risks of disclosure of personal information. Where possible, in these areas, computer equipment should not access systems containing personal information. Where this is not possible, no personal information should be stored on local PCs/Laptops and a strict clear screen policy must be applied (see clear screen policy below).

6.0 Processes

6.1 Data/Information Labelling

In order to ensure that appropriate levels of security are applied in a consistent manner, all data and information must be appropriately labelled.

In the case of information contained within IT systems and databases, the system itself must be registered and, where possible, reminders of the Information Classification should be displayed on screens e.g. 'This system contains personal information that is classified as 'Official – Sensitive'. Please be reminded to maintain the confidentiality of this information'. Any reports extracted from such systems must be appropriately labelled. Where it is not possible for a label to be printed, it should be handwritten on the first page.

All documents (e.g. MS Word, PDF documents etc.) must be clearly labelled (on the cover page and in headings/footers) with the information classification clearly labelled e.g. OFFICIAL – SENSITIVE, OFFICIAL – INTERNAL, PUBLIC etc.

The label must be in the format: ‘Data Label: Official - Internal’

For further information and advice on data/information labelling, please contact the council’s records manager.
6.2 Systems Access to Information

As a rule, all personal information should be kept within secure premises and systems.

Where it is not possible to access information on secure premises and systems, the following hierarchy should apply:

1. Access should be via secure remote access so that information can be viewed or amended without being permanently stored on remote computers.
2. Next best is secure transfer of information to a remote computer on a secure site on which it will be permanently stored.
3. Decisions on handling/transfer of information should be approved by the relevant asset owner.
4. User rights to transfer information to removable media must be limited to secure, approved methods ONLY.

For all systems containing personal information, strong passwords must be used, as per the council’s password policy. This may be viewed on the council’s Intranet or by following this link: Password Policy.

More robust ‘two-factor’ authentication methods are required for particularly sensitive data sets or high risk environments. The requirement for these devices (that include RSA Tokens) will be determined as an outcome of a privacy impact assessment.

An example of where token access may be required is where case officers are accessing secure back-end systems (containing protected information) from remote locations.

Hard passwords (network passwords) are secure enough for general remote access to email (web mail) facilities.

6.3 Mobile Devices/Removable Media (Laptops etc.)

All services must consider the specific risks of using removable media including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats.

Ideally, the use of removable media (including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats) should be avoided for storage or access to such data. However, it is recognised that is not possible to avoid altogether the use of removable media, but following conditions MUST be applied:

- Unencrypted USB Memory Sticks must never be used for the storage or transfer of personal information within West Lothian Council.
- All Laptops used in high-risk areas and/or where sensitive personal and Protect information is used, must be encrypted (to Council Standards).
- Mobile Phones, MP3 Players and other personal equipment must not be connected to council IT equipment. The only exception to requirement is in a supervised classroom (school) environment.
• Mobile Phones, MP3 Players, SD Cards and other Media Cards must not be used for the storage or transfer of any personal or Protected Information.

• The use of removable disks, CDs and DVDs should only be considered once it is established that more secure methods of transfer are not available. They should not be used for the transfer of personal or Protected information.

• Council owned PDAs, Blackberrys and Smart phones should not be used for the storage or transfer of sensitive information. All such devices must be encrypted and password protected with facilities and procedures in place for the remote wiping of data should the device be lost.

User rights to transfer data to removable media should be carefully considered and strictly limited to ensure that this is only provided where absolutely necessary. Additional Staff awareness training, follow up training and guidance will be required in areas where mobile devices/removable media is in operation.

Even under controlled conditions, the information transferred to any removable media should be the minimum necessary to achieve the business purpose, both in terms of the numbers of people covered by the information and the scope of information held.

6.4 Email

Personal Protected information should never be sent over normal email systems. Where it is necessary to send such mail, it must always be encrypted.

Email sent via the GSx and from the Council to Lothian NHS Trust does not travel over the public Internet and special arrangements are in place to secure such email.

No council email should be sent to any staff personal home user accounts e.g. Hotmail, Yahoo Mail, Googlemail, BT etc. This is in strict breach of the council’s Information Security Policy. Where staff need to work from email accounts from outside the council network, secure access to council email accounts can be arranged (contact IT services).

The email system should never be used for the bulk transfer of data between the council and external bodies (especially personal information). Secure file transfer methods should be used for such purposes. For further advice on secure file transfer, contact the Information Security Officer: InfoSec@westlothian.gov.uk.

6.5 Transfer/Sharing of Information (information in transit)

All transfers of information out of West Lothian Council networks/Systems e.g. bank transfers etc. must be conducted using secure connections e.g. VPN (Virtual Private Network), SFTP (Secure File Transfer Protocol) and SSL (Secure Socket Layer) technologies.

Such information transfers must not be conducted using traditional mail methods e.g. posting CDs, memory sticks, database reports etc. Secure file transfer methods must be used for such purposes. For further advice on secure file transfer, contact the Information Security Officer: InfoSec@westlothian.gov.uk.

All transfers must be pre-arranged. If in doubt, please contact the IT Service Desk: itservicedesk@westlothian.gov.uk

Data Label: Official
Information sharing outwith West Lothian Council (public or private organisations) is strictly forbidden unless particular information sharing protocols and third party access agreements have been put in place e.g. C-Me. If in doubt, please contact line managers in the first instance.

6.6 Storage of data/information (information at rest)

All personal information must be stored on central systems and not permanently stored on PCs, Laptops or any other removable media. This ensures complete data sets are available, appropriate security access levels can be applied, critical information is backed up and that appropriate disaster recovery arrangements can be put in place. For the same reasons, all documents should be stored on the council’s EDRM or on secure network drives where EDRM is not available.

It is recognised that information ‘in transit’ may be temporarily stored on different forms of removable media. However, all media should be secured (including encryption) to minimise the risk of damage, loss or unauthorised disclosure of information.

6.7 Faxing, Printing and Copying

Particular care must be taken not to leave copies of Protect, Personal or otherwise sensitive information on fax machines, printers and photocopiers.

Faxing is less secure than other methods. All staff must be aware of this before faxing personal information.

Incoming faxes should be directed to automatic mail accounts for distribution. If in doubt, please contact the IT Service Desk: itservicedesk@westlothian.gov.uk.

Outgoing faxes must contain the minimum of personal information and the sender should seek confirmation of delivery with the addressee.

6.8 Testing

To ensure the correct levels of security are maintained it may be necessary to have high-risk systems tested (on at least an annual basis). Such tests are normally conducted by external consultants e.g. penetration testing and ‘Code of Connection’ testing. Live data must not be used for testing and must not leave the council network or systems.

‘Anonymised’ data sets must be used for testing new systems or changes to systems containing ‘Protected’ Information.

6.9 Privacy Impact Assessments

The introduction of new systems and major developments in existing systems will warrant ‘Privacy Impact Assessments’*. Privacy Impact Assessments are supported by the Information Commissioner and are “…a process whereby a project’s potential privacy issue and risks are identified and examined from the perspectives of all stakeholders and a search is undertaken for ways to avoid or minimise privacy concerns”

6.10 Third Party Access

Where third party access is required e.g. for systems support or information sharing, the third party must sign up to an approved ‘Third Party Access Agreement’. This will ensure non-disclosure of information and that an equivalent level of security and scrutiny is applied to West Lothian Council data.

6.11 New ICT Systems and Information Security Tools

For new systems containing personal information, the council must aim to have systems accredited to Government standards. It must be made a condition of supply that suppliers and contractors adopt equivalent levels of security when delivering their services. The current standard for ‘Protected’ information is managed by the UK Government’s ‘Communications Electronic Security Group’ (CESG). The CESG Claims Tested Mark (CCTM) and Assisted Product Service (CAPS) schemes provide a government quality mark for the public and private sectors based on accredited independent testing, designed to prove the validity of security functionality claims made by vendors. In more colloquial terms, the CCTM and CPAS are designed to assure public bodies that a product or service does ‘what it says on the box’.

The American equivalent to this, FIPS (Federal Information Processing Standards) is widely used for suppliers based in the USA.

6.12 Clear Screen Policy

All PCs, laptops, workstations etc. must always be ‘locked’ when unattended. The can be locked using the standard keyboard combinations:

‘CTL-ALT-DEL’ then’ Lock Computer’ or

‘Windows’ Key + L.

This ensures that information cannot be viewed and is password protected from unauthorised access.

6.13 Risk Management

Information Management risks are to be managed as per the council’s Risk Management procedures and guidance. Please follow links (below) for more information:

Risk and Insurance Intranet Page

Risk and Insurance Contacts
### Summary of Information Handling Requirements by Classification

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Security Marked</th>
<th>Official - Sensitive</th>
<th>Official - Internal</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Information on the Council’s Personal Information Register</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Not required</td>
<td>Not Required</td>
</tr>
<tr>
<td>Entry on Risk Register with Risk Analysis</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>System Owners Assigned</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>Check Data Protection Registration</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>Information Classifications required</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Staff need to be aware of Information Security Policy</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Staff Information Security Awareness Training</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Specific Local Guidance</td>
<td>Mandatory</td>
<td>May be required in high risk areas</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>Incident Reporting</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>User Access Rights –Passwords</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Token Access (e.g. RSA Tokens)</td>
<td>Mandatory</td>
<td>May be required in high risk areas</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>ID Cards</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Clear Desk/Screen Policy</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Required for public places</td>
<td>Recommended</td>
</tr>
<tr>
<td>Visitor Recording/Accompanying</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Recommended</td>
<td>Not Required</td>
</tr>
<tr>
<td>Paper Records Locked Away</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Recommended</td>
<td>Not Required</td>
</tr>
<tr>
<td>Laptops Locked Away</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Removable Media Locked Away</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Conversations Not overheard</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Not Required</td>
</tr>
<tr>
<td>Shredding of documents</td>
<td>Mandatory</td>
<td>Documents may be shredded</td>
<td>Documents may be shredded</td>
<td>Documents may be recycled (without shredding)</td>
</tr>
<tr>
<td>Secure Disposal of documents</td>
<td>Mandatory</td>
<td>Highly sensitive documents may require secure disposal</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>Secure disposal and reuse of IT equipment</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>USB Drives</td>
<td>Not Permitted</td>
<td>Only Council Standard Encrypted Devices Permitted</td>
<td>Council Standard Encrypted devices recommended</td>
<td>Council Standard Encrypted devices recommended</td>
</tr>
<tr>
<td>Mobile Devices</td>
<td>Not Permitted</td>
<td>Only to be used with Council approved security conditions in place</td>
<td>Only with Council approved security conditions in place</td>
<td>Recommended</td>
</tr>
<tr>
<td>Data Labelling</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td></td>
<td>Security Marked</td>
<td>Protect</td>
<td>Internal</td>
<td>Public</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------</td>
<td>--------------------------------------------------------------</td>
<td>-----------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Remote Access</td>
<td>Not Permitted</td>
<td>Only to be used with Council approved security conditions in place</td>
<td>Secure methods only</td>
<td>Recommended</td>
</tr>
<tr>
<td>Email</td>
<td>Not Permitted</td>
<td>Only encrypted email to be used</td>
<td>Limit to internal mail accounts</td>
<td>No limitations</td>
</tr>
<tr>
<td></td>
<td>(unless GSX/GSI email)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td>Not recommended</td>
<td>Only on security protected networked systems and EDRM)</td>
<td>EDRM and Host applications</td>
<td>EDRM and Host Applications</td>
</tr>
<tr>
<td></td>
<td>on Council Systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Faxing</td>
<td>Not Permitted</td>
<td>Not Permitted</td>
<td>Not recommended</td>
<td>No limitations</td>
</tr>
<tr>
<td>Printing and Copying</td>
<td>Express permission of owner required</td>
<td>Express permission of owner required</td>
<td>Not recommended</td>
<td>No limitations</td>
</tr>
<tr>
<td>Security Testing</td>
<td>Mandatory</td>
<td>Required on an annual basis</td>
<td>Required on an annual basis</td>
<td>After change/Update</td>
</tr>
<tr>
<td>System Testing</td>
<td>Mandatory</td>
<td>Only Anonymised information to be used. Live testing must not be conducted.</td>
<td>After each change/Update</td>
<td>After each change/Update</td>
</tr>
<tr>
<td>Privacy Impact Assessment</td>
<td>Mandatory</td>
<td>Mandatory for new developments and significant changes</td>
<td>Mandatory for new developments and significant changes</td>
<td>After each change/Update</td>
</tr>
<tr>
<td>3rd Party Access Agreements</td>
<td>Not Permitted</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Not Required</td>
</tr>
<tr>
<td>Government Standard (CESG)</td>
<td>Mandatory</td>
<td>Mandatory</td>
<td>Recommended</td>
<td>Recommended</td>
</tr>
</tbody>
</table>