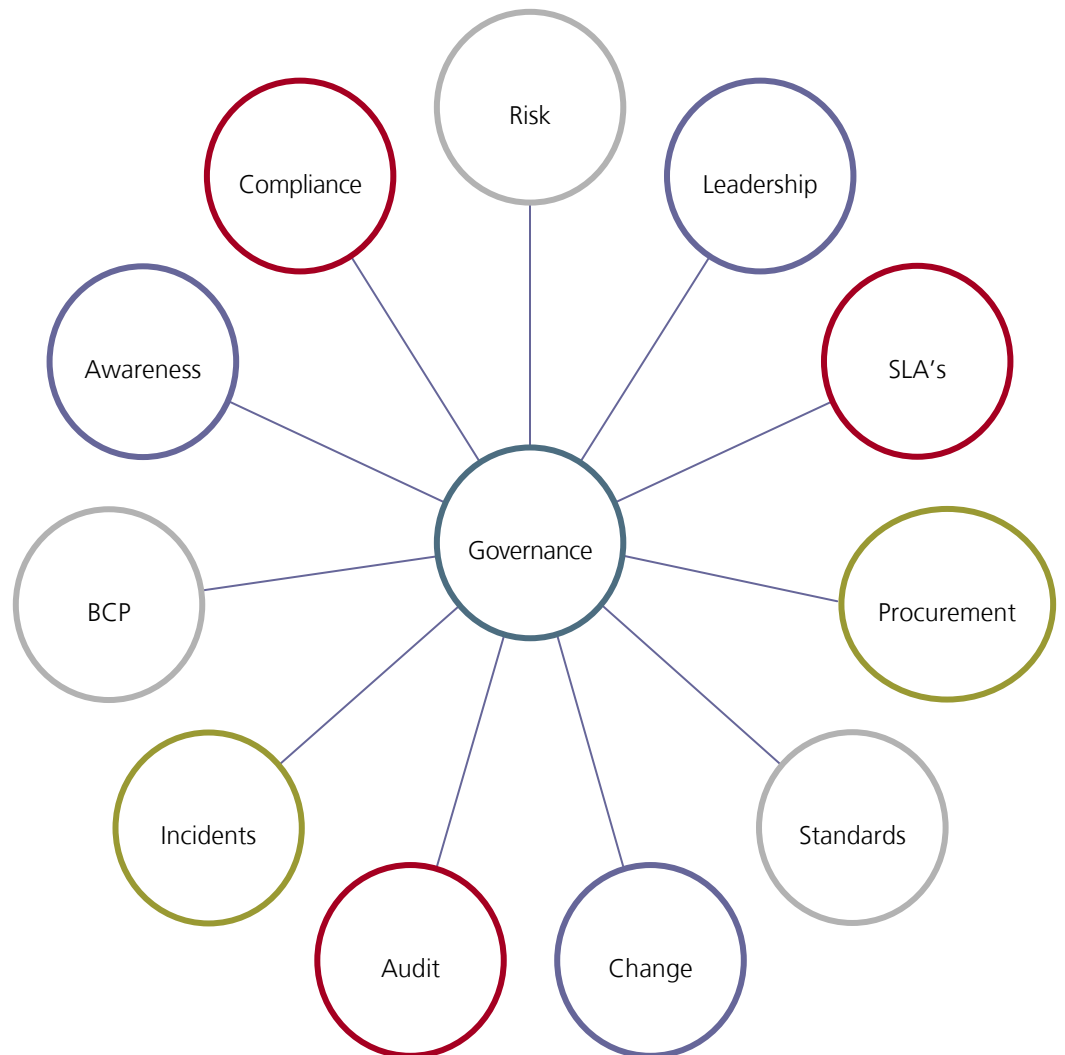




Local Government

Data Handling

Guidelines



Foreword

People rightly demand high standards from public services. In practice, this may mean the customer providing personal details once, quite possibly via the web, to unlock a set of services sourced from a series of different providers. So, an elderly person requiring support from care and health services should not be faced with an off putting and complex array of forms, systems and officials to access help.

This is at the heart of what councils strive to do. Success depends on many factors, but an essential underpinning is effective use and exchange of information both within councils and between councils and other services such as health and education. It is therefore crucial that the public has confidence that any data they provide is treated with appropriate confidentiality and kept safe from any risk of misuse.

Recent losses of personal data such as that from Her Majesties Revenue and Customs require that all public bodies act to bolster public trust and confidence in the way personal information is handled and kept safe.

These guidelines are a response to that need. They set out the fundamental steps that every council should take to mitigate against the ever present risk that personal information is lost or that data protection systems fail. They therefore provide chief executives, senior managers and elected members with a vital aid in discharging their responsibilities and accountability for secure and effective handling of personal information.

The guidelines were prepared by working closely with councils to meet local government circumstances. They were also worked up in close co-operation with central government because councils need to work with a very wide range of public bodies and therefore to exchange information for legitimate and often essential reasons in the interests of providing effective services.

Behind the guidelines will be a growing resource of more detailed help and information. I am sure that robust application of the guidelines coupled with the characteristic vigilance of councils will minimise the risks in handling personal data that we all know is present in our day to day work in serving the public

Paul Coen, Chief Executive, Local Government Association

And Steve Thomas; Chief Executive, Welsh Local Government Association

Local government is a primary interface between government and the general public. Following the publication of my Data Handling Procedures in Government: Final Report earlier this year, I am very pleased to see that local government is taking similar steps to protect the personal information it handles.

Modern, effective public services rely on public bodies sharing information in order to provide a better and more joined up service for our customers. I therefore welcome these guidelines and the partnership they represent between central and local government. Rightly, they are designed to meet the business needs and circumstances of councils yet they also complement and are consistent with guidelines prepared for central government and their agencies.

We are working hard in central government to achieve a culture change where all those who handle data on behalf of government treat it as a most valuable asset and protect it as such. This guidance will help to achieve the same kind of understanding and commitment to improving data security across the whole of the public sector.

Sir Gus O'Donnell, Cabinet Secretary

I welcome these guidelines as a significant step towards ensuring the consistent, proportionate and secure use of personal information by government at all levels

They make an important contribution to the aim of the Information Commissioner's Office that all organisations should inspire trust by collecting and using personal information responsibly, securely and fairly. In investigating any apparent breaches of the Data Protection Act by councils we will look to see whether these guidelines have been implemented effectively and take this into account in assessing whether councils are meeting their obligations.

I believe that if councils effectively implement the steps set out in the guidelines, they will significantly reduce the risk of incidents and problems, and in doing so, help build the necessary public trust in the handling of personal information that recent and well publicized incidents can only have eroded.

Richard Thomas, Information Commissioner

Acknowledgements

The LGAWLGA would like to thank all those from Central and Local Government who provided valuable advice and support and contributed to this work, in particular Mark Brett, Socitm.

Background

Information: a key business asset and fundamental to the delivery of public services – are you doing enough to protect the data entrusted to you?

The drive to improve public services demands that the public sector delivers services in ways that bring benefits to citizens, staff and taxpayers alike; it is only through the better use of information and data sharing that councils will be able to provide efficient services that meet this objective.

Following the high profile loss of data by HM Revenue and Customs public confidence in Government's, and thus the wider public sector's, ability to securely protect its information is at an all time low. Therefore, if councils are to deliver more efficient personalised services they need to rebuild public confidence that they will protect their privacy and use and handle their information professionally.

In November 2007, the Cabinet Secretary, Sir Gus O'Donnell was asked to review the Government's procedures for data handling and in June 2008 published 'Data Handling Procedures in Government'¹. The Cabinet Office guidance focuses on central Government bodies but recognises the crucial role of local councils and thus the Local Government Association (LGA) and the Welsh Local Government Association (WLGA) agreed to lead on producing equivalent standards for local government.

This document recognises that councils are best placed to assess their own risk and put in the necessary safeguards and therefore this guide aims to serve as a checklist, highlight best practice and provide reference to useful resources whilst acknowledging that councils will often have their own standards which are equivalent to, or exceed, those set out in this document.

A lot of excellent work has already been done but there is still more to do; the pace of technological development means that councils need to be ever aware of new risks and threats.

Scope

As with the 'Data Handling Procedures in Government'¹ report "...this report considers both use of data within a given organisation and use of when data are shared, but does not seek to explore issues specifically around data sharing. The work considers how data can be kept safe and how it should be handled, rather than whether sharing of particular data in a particular way is desirable. "

A review of data sharing² in the UK public and private sectors led by Richard Thomas, the Information Commissioner and Dr Mark Walport, Director of the Wellcome Trust, has recently been published.

The material in this document reflects good practice as set out in the ISO/IEC 27000 (Information Security Management System) series and is also aligned with Central Government Information Assurance policy, produced by CESG (the Communications and Electronic Services Group, part of GCHQ).

¹ Data Handling Procedures in Government <http://www.cabinetoffice.gov.uk/csia>

² Data Sharing Review <http://www.justice.gov.uk/docs/data-sharing-review-report.pdf>

The guidance is not exhaustive and relies upon other initiatives, legislation and processes for completeness - these include:

- Data Protection Act
- Human Rights Act
- Freedom of Information Act
- Crime and Immigration Act
- Civil Contingencies Act
- Government Connect Code of Connection

It is envisaged that following the publication of this guidance the LGA and WLGA, with key stakeholders from across the public sector, will look to create a resource and service to aid councils in addressing this challenge.

Structure

The standards that local government is setting itself in this document are challenging but necessary to rebuild public confidence. If we are to meet this challenge it will only be through first, creating the right culture, and second, by having the right policies and procedures in place to provide accountability and scrutiny. Therefore, the core of this report is structured around four headings:

- people
- places
- processes
- procedures

No council can ever say it will never lose information but by ensuring the standards in your council are equivalent to, or exceed, the best practice identified in the each of the sections, the public will be reassured that all reasonable steps were taken to preserve and protect their information.

Following the specific checklist of best practice there are two further sections: 'Top 10 Data Handling Tips' produced by the Society of Information Technology Management, and Useful Resources.

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

✔ *Appoint a Senior Information Risk Owner (SIRO) to ensure there is accountability*

The SIRO should be a senior manager who is familiar with the information risk and the organisation's response. They should provide written judgement of the security and use of the business assets at least annually to support the audit process and provide advice to the accounting officer on the content of their statement of internal control.

✔ *Each system should have an Information Asset Owner*

These are Business Managers who operationally own the information contained in their systems. 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 within an acceptable level of risk.

✔ *Identify Users and their access rights*

Asset Owners should regularly review user access rights. Users are those staff, contractors and suppliers who access and process sensitive personal information for and on behalf of the council. By default, no member of staff should have access to systems containing personal protected information. Where access is deemed

necessary, it should be to the smallest possible sub-set of records.

✔ *Foster a culture that properly values, protects and uses information*

Councils should have and execute plans to lead and foster a culture that values, protects and uses information for the public good.

- Ensure awareness raising and training is conducted at the appropriate level and monitor understanding and ability periodically; regular updates should be scheduled for all employees.
- Create and enforce Human Resource policies around information management, in particular making clear that failure to apply the council's procedures is a serious matter and in some situations, can amount to gross misconduct.

✔ *Maintain mechanisms for reporting and managing information risk incidents*

- Develop mechanisms through which individuals may bring concerns about information risk to the attention of senior management.
- Ensure the council is a member of the Regional Local Authority WARP³ (Warning, Advice and Reporting Point) or the equivalent group in Wales. A WARP is a community-based service where members can receive and share up-to-date advice on information security threats, incidents and solutions.

³ Local Authority WARP (Warning, Advice and Reporting Point) www.nlawarp.gov.uk

✔ *Maximising public benefit*

The council, and specifically the Information Asset Owners, should consider how better use could be made of their information assets within the law. Councils should consider how public protection and public services can be enhanced through greater access to information held by others.

✔ *Publish an information charter*

All councils should publish an information charter setting out how they handle information and how members of the public can address any concerns that they have. A sample charter is available in the 'Data Handling Procedures in Government'⁴ report.

Places – All councils should ensure the security of their information through the physical security of their buildings, premises and systems. There should be regular assessments of information risks, which are discussed by senior management.

✔ *Undertake regular risk assessments*

Councils should undertake regular risk assessments to ensure confidentiality, integrity and availability of the information they hold. There should be clear records of the assessments conducted and these should be shared and discussed with senior management.

✔ *Ensure buildings and premises are secure*

- Issue all staff with ID cards, ensure that they are worn and challenge people that are not wearing them.
- Record all visitors to buildings and wherever feasible ensure that they are accompanied whilst on the premises.

- Implement a clear desk/clear screen policy to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours or when areas are unattended.
- Ensure where personal information is held on paper, it is locked away when not in use or the premises are secured.

✔ *Ensure the secure disposal of information.*

All personal information should be securely destroyed: paper records by incineration, pulping or shredding so that reconstruction is unlikely and electronic media by overwriting, erasure or degaussing for re-use. This is in accordance with government guidelines. Where possible, a CCTM⁵ approved product or service should be used.

✔ *Wherever possible, avoid the use of removable media*

Wherever possible councils should avoid the use of removable media including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats. Where it is unavoidable, encryption⁵ should be used and the information transferred should be the minimum necessary to achieve the business objective.

Processes – All councils should check that they have proper document systems in place and that their suppliers and contractors, when handling their information, work to the same standards. Councils should also monitor and audit the effectiveness of their policies and, where appropriate, engage independent experts to test ICT systems and make recommendations.

✔ *Work towards a policy of least privilege*

⁴ Data Handling Procedures in Government
<http://www.cabinetoffice.gov.uk/csia>

⁵ CESG Claims Tested Mark (CCTM),
<http://www.cctmark.gov.uk/>

Wherever possible, access to systems should be restricted to those users that need it. Access to raw data should be strictly controlled and where possible, only anonymous data should be readily available. Use of the cross-government Employee Authentication Service ⁶ is an option which should be considered.

✔ 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:

- Access should be via secure remote access so that information can be viewed or amended without being permanently stored on the remote computer.
- Next best is secure transfer of information to a remote computer on a secure site on which it will be permanently stored.
- Decisions on handling/transfer of information should be approved in writing by the relevant information asset owner.
- User rights to transfer information to removable media should be carefully considered and strictly limited.

✔ Wherever possible, the bulk transfer of information should be carried out via a secure network

Where it is necessary to bulk transfer information, it should be done electronically across the secure Corporate Network. Where information needs to be shared between organisations, the GCSx (Government Connect⁷) should be used wherever possible. This will facilitate the

⁶ Employee Authentication Service
<http://www.dcsf.gov.uk/localauthorities/>
⁷ Government Connect
<http://www.govconnect.gov.uk/>

transfer of information across the wider GSI and interlinks with other secure Government Networks: Connection, Health, Criminal Justice and others. It is never acceptable to transfer bulk personal information via normal email services.

✔ Engage independent experts to carry out penetration testing

All councils should engage independent experts who are members of a TigerScheme, Crest, or CHECK to carry out penetration testing of all ICT systems where it is deemed necessary.

✔ Conduct Privacy Impact Assessments

Where appropriate conduct Privacy Impact Assessments⁸ for new systems being implemented. Privacy Impact Assessments are supported by the Information Commissioner and are "...a process whereby a project's potential privacy issues 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..."

✔ New ICT systems should be accredited to Government standards

For new systems containing personal information, councils should aim to have systems accredited to Government standards. When procuring new systems, councils should also consider putting in place arrangements to log activity of users in respect of protected personal information and for asset owners to check it is being properly conducted.

✔ Ensure that your suppliers and contractors adopt equivalent standards

⁸ Privacy Impact Assessments Handbook
http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/foreword.html

When suppliers and contractors are handling information on behalf of the council, then the council should mandate equivalent standards where they can and seek to influence others where they cannot mandate.

Procedures – All councils should produce a Corporate Information Risk Policy which sets out how they will implement the measures in this document, as well as produce policies for risk reporting and risk recovery. They should ensure that there are mechanisms in place to test, monitor and audit the policies and procedures of the council.

✔ *Produce a Corporate Information Risk Policy*

The policy should set out how to implement the measures in this document in relation to councils activities and that of delivery partners, and monitor compliance with the policy and its effectiveness.

✔ *Complete Corporate Information Risk Plans (review and forward looking)*

At least once a year complete a Corporate Information Risk Plan, review all assessments and examine forthcoming potential changes in services, technology and threats.

✔ *Produce a Risk Recovery Policy*

Councils should have a policy for recovering from information risk incidents. This includes losses of protected personal data and ICT security incidents. The policy should cover the council's media and legal response, and should have clearly defined responsibilities; all staff should be made aware of the policy.

✔ *Risk reporting mechanisms*

Security incidents should initially be reported to the Regional Local Authority

WARP⁹ or the equivalent group in Wales, and for serious network security incidents, to GovCERTUK¹⁰. Significant, actual or potential losses of personal information should be shared with the Information Commissioner's Office¹¹.

✔ *Regularly test your policies and procedures*

Councils should regularly test their policies and procedures; this should include a range of measures from testing awareness and understanding of policies among staff, to testing the implementation of specific procedures such as correct use of encryption, appropriate user rights, use of removable media and correct disposal of information.

Socitm's Top 10 tips for Data Handling

1. Ensure you understand which legislation affects your business area.
2. Ensure a named individual in the business, not ICT, owns the risk.
3. Ensure there is an effective incident reporting mechanism in place.
4. Regularly monitor, measure and audit your processes and procedures.
5. Establish a Corporate Information Governance group.
6. Ensure all staff are trained, updated and aware of their responsibilities.
7. Undertake regular risk reviews of all processes and procedures.
8. Ensure all key information assets are classified and are resilient.
9. Have robust risk driven processes in place for "ad hoc" situations.
10. Have documented policy driven processes and procedures in place.

⁹ Local Authority WARP (Warning, Advice and Reporting Point) www.nlawarp.gov.uk

¹⁰ CESH's Incident Response team (GovCertUK) <http://www.govcertuk.gov.uk/>

¹¹ The Information Commissioner's Office <http://www.ico.gov.uk/>

Useful resources

- *The Information Commissioner's Office* <http://www.ico.gov.uk/>

The ICO enforces and oversees the Data Protection Act, the Freedom of Information Act, the Environmental Information Regulations, and the Privacy and Electronic Communications Regulations. They provide information and advice, and their website contains useful sources of best practice documentations and practitioner guides.

- *WARP (Warning, Advice and Reporting Point)* <http://www.nlawarp.gov.uk>

Regional Local Authority WARPs are community-based services where members can receive and share up-to-date advice on information security threats, incidents and solutions.

- *The Employee Authentication Service* <http://www.dcsf.gov.uk/localauthorities/>

The employee authentication services (EAS) is a scalable, sustainable, secure solution that will enable employees in central and local government, schools and other organisations to access and share sensitive information in order to improve services for the benefit of children, learners and citizens.

- *The National Technical Authority for Information Assurance, CESG* <http://www.cesg.gov.uk/>

CESG aims to protect and promote the vital interests of the UK by providing advice and assistance on the security of communications and electronic data. They deliver information assurance policy, services and advice that government and other customers need to protect vital information services.

- *CESG's Incident Response team (GovCertUK)* <http://www.govcertuk.gov.uk/>

GovCertUK provides CESG's CERT function to UK government and the wider public sector. Their role is to assist public sector organisations in responding to computer security incidents and provide advice to reduce exposure to threat.

- *CESG Claims Tested Mark (CCTM)* <http://www.cctmark.gov.uk/>

The CESG Claims Tested Mark (CCTM) scheme provides 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.

- *Standards to aspire to: ISO 27001 and Government Connect Code of Connection*

The work towards achieving compliance with the Government Connect Code of Connection will help with achieving ISO 27001 compliance. It must be noted, however, that compliance with the Government Connect Code of Connection is not an end in itself.

- *The Devon Information Security Partnership (DISP) Security framework is a recommended approach for implementation*

The Devon Information Security Partnership (DISP) is a comprehensive framework, based on ISO 27001, which is freely available to all Local Councils under a GNU Open Source licence, to assist with implementing information security measures.

- *The SOCITM e-service delivery standard for ICT is a good maturity model to track progress towards compliance with the guidelines*

The Socitm NeSDS (ICT) Guidelines offer a comprehensive maturity modelling approach to ICT service delivery. The standard includes elements around security and resilience (Business Continuity).

Local Government Association
Local Government House
Smith Square, London SW1P 3HZ

Telephone LGconnect,
for all your LGA queries, on 020 7664 3131
Fax 020 7664 3030
Email info@lga.gov.uk
Website www.lga.gov.uk

ISBN: 978-1-84049-650-5
F/SR274
© LGA, November 2008



Local Government Association

The Local Government Association is the national voice for more than 450 local authorities in England and Wales. The LGA group comprises the LGA and five partner organisations which work together to support, promote and improve local government.

