Local public services data handling guidelines

Guidance
August 2012
version 2

Acknowledgements

Through the NLAWARP initiative, a number of Local Authority and other colleagues have contributed to this revised edition;

- Dave Sifleet, LB Brent
- Bruce Thomson, LB Hillingdon
- Dave Thomas, LB Havering
- John Finch Plymouth, City Council
- Roheren Evans, Conwy County Council
- Andrew Durrant, Powys county Council
- Kelly Waterfield, Denbighshire County Council
- John Bagley, London PSN
- Richard Roscoe Sefton MBC
- Chris Pounder, Amberhawk Associates
- James Wood, Connecting for Health
- Arwyn Morris, Ceredigion County Council
- Principal Author: Mark Brett Programme Director NLAWARP

PSN Supporting Statement

I welcome the revised Local Public Services Data Handling Guidelines. This guidance provides valuable information to organisations connecting to, and consuming services across, the Public Services Network (PSN). To maximise the benefits of the shared public sector infrastructure it is essential that we achieve common trust built on a common set of standards, and therefore every organisation must exercise a corporate approach to Information Risk Management and Information Governance. This guidance offers an approach compatible with the PSN Security Model and Planting the Flag, the Local Public Services response to the Government ICT Strategy. Finally this guidance assists organisations in complying with the PSN Information Assurance Conditions – an essential step in connecting to the shared public sector environment.

John Stubley Operations Director, PSNA

Foreword

People continue to demand higher standards of public services, wanting easier access to services and a 'one-stop shop' delivery experience. They want to be in control of their interaction, and for services to be delivered at lower cost, more quickly and based on their specific needs.

In practice, this will increasingly require, for example, 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 each item for which they need help.

This lies at the very core of what all local public services strive to do. Success depends on many factors, but effective and secure exchange of information is vital. This exchange is typically needed both within and between councils as well as with other services such as health and education. For this to be possible it is crucial that the public has confidence in the way that any data they provide is treated, taking privacy and confidentiality into account, and that it is kept safe from misuse.

Yet, data continues to be lost or disclosed resulting in fines from the Information Commissioner's Office and loss of public trust. It is a legal requirement under the Data Protection Act to ensure that personal information is properly protected. The Public Services Network, Government Connect and Connecting for Health (N3 Network), all require this protection to be in place, and all public bodies must pay sufficient attention to the way personal information is handled and kept safe.

These guidelines are a response to these needs. They set out the steps that every council should take to monitor, control and to mitigate the risk should personal information be lost or data protection systems fail. They seek to support chief executives, senior managers and elected members in discharging their responsibilities and accountability for the secure and effective handling of personal information.

The guidelines were prepared by working closely with the Local CIO Council, Socitm, the Cabinet Office and the NLAWARP. They were developed in close co-operation with central government and other public bodies recognising that councils need to work with a wide range of public bodies in the interests of providing effective services, and also recognising the need to exchange information with others for legitimate and often essential reasons.

Behind the guidelines will be a growing resource of more detailed help and guidance for information professionals and others, forming part of the 'Planting the Flag Strategy' for IT-enabled local public services. We are sure that robust application of the guidelines coupled with the characteristic vigilance of councils will help to reduce the risks associated with handling personal data.

Jos Creese, Chair - Local CIO Council
CIO Hampshire County Council

Kay Brown, President, Socitm
Head of ICT in South Lanarkshire Council

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?

Protecting personal information is a legal requirement under the Data Protection Act 1998. The Information Commissioner's Office now has a range of enforcement actions including the power to fine organisations up to £500,000.00 for non-compliance; the Information Commissioner regularly issues fines of around £100,000.

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

Following the high profile losses of data by public sector organisations confidence in the public sector, is at an all time low. Many of the data losses have been wholly preventable, being the result of careless administrative procedures.

Therefore if Local Public Services are to deliver the efficient, personalised, and often shared services that they aspire to, they will need to build public confidence and ensure that the public feel their privacy is protected and their personal information is handled 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'. The Cabinet Office guidance focuses on central Government bodies but recognises the crucial role of Local Public Services - thus the Local Government Association (LGA) and the Welsh Local Government Association (WLGA) agreed to lead on producing equivalent standards for local government. Since then there have been a number of changes in infrastructure and the general approach to Information Assurance.

This updated version of the Local Government Guidance reflects those changes and highlights the progress made. We acknowledge that there has been progress. However, the number of fines issued by the ICO to local public service organisations clearly demonstrates that there is still some way to go. This document develops an approach to help organisations to move towards an Information Governance regime that is fit for purpose for a Public Services Network (PSN) environment.

This document recognises that ***Local Public Services are best placed to assess their own risk and put in place the necessary safeguards***. It therefore aims to serve as a check list, highlighting best practice and referencing useful resources whilst acknowledging that Local Public Services will often maintain standards which are equivalent to, or exceed those set out in this document. The Government's Security Policy Framework (SPF) is not mandated for Local Government, but it is relevant. The recent version 7 has reduced the number of minimum measures from

70 to just 20. This guidance covers the essence of those measures and their applicability in a Wider Public Sector (WPS) environment. A lot of excellent work has already been done but there is still more to do; the pace of technological development means that Local Public Services need to be ever aware of new risks and threats.

Scope

As with the `Data Handling Procedures in Government' report, this report considers both use of data within a given organisation and the use of data when shared. It 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.

The material in this document reflects good practice as set out in the ISO/IEC 27000 (Information Security Management) series and is also aligned with Central Government Information Assurance policy, produced by CESG (the National Technical Authority for Information Assurance, part of GCHQ). The government policy document covering these areas is known as IAS6 “Protecting Personal Data and Managing Information Risk”. This document forms part of the HMG Security Policy Framework (SPF), which details 20 mandatory measures for Government Organisations.   There is supporting guidance and documentation as part of the Public Services Network (PSN) Information Assurance Conditions, available from the PSN part of the Cabinet Office website. This guidance also forms part of that document set. The PSN Security Model gives an overarching view of the philosophy and approach to information assurance and risk management for the PSN. All Information Assurance requirements for the PSN are based around the basic technical controls of ISO 27001. This data handling guidance builds on those controls as specialist advice for Local Public Services. The key requirement is to ensure an ISMS (information Security Management System)and a corporate information security policy exists.

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

- Data Protection Act (DPA)
- Human Rights Act (HRA)
- Freedom of Information Acts in the UK (FOIA and FOISA)
- Crime and Immigration Act
- Civil Contingencies Act
- HMG Security Policy Framework (SPF)
- Government Connect Code of Connection
- Public Services Network (PSN) Information Assurance Conditions
- Connecting for Health Information Governance Tool-kit (IGT) for Adult Social Care
- The N3 (NHS) Information Governance Statement of Compliance, (IGSOC)

- Wales Accord for Sharing of Personal Information (WASPI)
- PSN Operational Security Architecture
- PSN Security Model
- PSN IA Conditions “Top-ups” for Health & Police Information

Structure

The standard that Local Public Services are setting themselves in this document is challenging but necessary to maintain public confidence.

If Local Public Services 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 five headings:

- Policy
- People
- Places
- Processes
- Procedures

No public service organisation can ever say it will not lose information - but by ensuring the standards in your organisation are equivalent to, or exceed, the best practice identified in each of these sections, the public and the Information Commissioner’s Office (ICO) will be reassured that all reasonable steps were taken to preserve and protect their personal information.

Following the specific check list of best practice there are two further sections: ‘Top 10 Data Handling Tips’ produced by the Society of Information Technology Management and an Useful Resources section.

Policy

A comprehensive set of policies, should form the heart of any information governance regime. Policies need to monitored and audit, to ensure they are being effectively enacted.

Local Public Services should implement a range of security policies, to ensure compliance with the PSN, N3 and GCSx / GCF regimes. Examples of policies covering a wide range of topics are available on the G3CToolkit website - www.g3ctoolkit.net . These policies are freely available for Local Public Services organisations to download, customise and implement.

A minimum set of policies should cover:

- Acceptable usage policy
- End user awareness training
- E-mail usage
- Use & control of portable media
- Home & mobile working
- Secure document printing

- Manual (paper) document handling
- Handling of faxes
- Secure disposal and destruction
- Information asset valuation
- Risk management regime
- Protective marking
- Use of personal devices
- The use of encryption software
- Incident reporting
- Incident management
- Log management
- Intrusion detection
- System Access Control
- Configuration management and change control
- Business continuity management

People

All organisations should seek to develop a culture so that ALL staff (including staff of contractors) properly value, protect and use information for the public good. Local Public Services should reinforce that *information is a key business asset* and that its proper use is not simply an IT issue.

As services are delivered remotely and in time using personal devices, training and awareness raising will significantly increase in its importance. For those using mobile devices, contextual awareness training, is essential. The training needs to be backed up by policy and regularly audited and monitored.

There should be clear lines of accountability for all levels of staff throughout the organisation together with a programme of staff awareness raising - starting at induction but continually updated - on an annual basis, clearly setting out the expectations of staff.

Ensure all staff working remotely in the field, and from home, are appropriately trained

This becomes increasingly important as more staff are mobile and often work from home. Local Public Services are beginning to introduce “Bring Your Own Device to Work (BYOD)” or issuing staff with personal portable devices for data storage in the field and at home. Specific context awareness training is becoming essential.

Appropriate staff vetting and background checks, should be carried out a part of the recruitment process, especially where staff will be accessing government networks and personal data. The Centre for the Protection of National Infrastructure (CPNI) is the government authority responsible for providing advice relating to personnel, physical and information security to the national infrastructure. There is a lot of guidance material on the CPNI website (www.cpni.gov.uk). Staff vetting brings confidence to the people aspect of the information assurance process. Personnel security is also a vital component of any information risk management regime.

Governance roles and responsibilities

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

The Public Services Network (PSN), IA Requirements, assumes a SIRO is appointed and is accountable for Risk Management, within the organisation.

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.

This sits along with the appointment of other roles such as Information Asset Owners and Information Assurance/Security Manager. The Information Asset Owners should be clearly identified, and their responsibilities set in line with SIRO requirements. The Information Assurance/Security Manager should also have a reporting line to the SIRO.

The National Archives produces a SIRO Newsletter. All SIROs should be urged to register with the National Archives.

The Council Information Security Manager, to be CESG Certified (CCP)

The security manager should be appropriately qualified and hold recognised industry qualifications.

To ensure understanding of government and wider public sector security matters, they should hold, or be working towards a CESG certified professional certificate of competence.

Security Organisation in place

The Local Public Services must establish an appropriate framework of security management and organisation (supported with appropriate staffing and training) with clear lines of responsibility and accountability at all levels of the organisation. This must include a Board-level lead with authority to influence investment decisions and agree the organisation's overall approach to security.

Each system should have an Information Asset Owner

These should be Business Managers who operationally own the information contained in their systems. Their role should be to monitor the use of portable devices 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

Part of the corporate risk management regime is the understanding of information risk, including the threats to information, some of which can emanate from staff. Part of the role of Information Asset Owner is to identify and control the access to the information system.

Access to information needs to be controlled, audit and pro-actively managed. All of these aspects form part of an information risk management regime.

Users (in the context of 'sensitive personal information') are those staff, contractors and suppliers who access and process any information (e.g. sensitive personal data) for and on behalf of the Local Public Services. By default, no member of staff should have access to systems containing personal protected information without prior authorisation. Where access is authorised, such authorisation should be set to the minimum needed for staff to perform their authorised work functions. Information Asset Owners should regularly review all user access rights

When staff or contractors, leave, transfer or change roles, their system and security access all need to be reviewed and revoked where necessary.

Foster a culture that properly values, protects and uses information

Local Public Services/Councils should have, and execute, plans to lead and foster a culture that values, protects and uses information for the public good. Such a culture has to be embedded with ALL staff including ALL levels of management.

Local Public Services/Councils should also:

- Ensure awareness raising and training is conducted at the appropriate level. Audit and record who has been trained. Regular updates should be scheduled for all employees.
- Create and enforce Human Resource policies, starting with recruitment training and induction, around information management, in particular making clear that failure to apply the Local Public Services procedures is a serious matter and, in some situations, can amount to gross misconduct.
- Maintain mechanisms for reporting and managing information risk incidents; this includes reporting losses of personal data as soon as reasonably practicable.
- Develop mechanisms through which individuals may bring concerns about information risk to the attention of senior management; and also develop processes to demonstrate that those concerns are taken seriously.
- Ensure that the Local Public Service/Council is a member of the Regional Local Authority WARP (Warning, Advice and Reporting Point) or the Cymru WARP in Wales. (As of July 2012, we are still trying to establish WARPs in Scotland and Northern Ireland.)

It is strongly recommended that a Corporate Information Governance Group (CIGG), chaired by the SIRO, is established. The CIGG should report back to senior management on a regular basis, at least quarterly.

Maximising public benefit

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

The exploitation of Public Information is a good catalyst for driving transformation and efficiency.

Publish an information charter

All Local Public Services 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 Cabinet Office `Data Handling Procedures in Government' report. There are also numerous examples on various local public service websites.

Sources of help and assistance

On behalf of the Cabinet Office, the National Archives is now providing free SIRO training to all Local Public Services. Contact: IATraining@nationalarchives.gsi.gov.uk.

The National Archives are also producing a SIRO Newsletter. All SIROs are urged to register with the National Archives.

A WARP is a community-based service where members can receive and share up-to-date advice on information security threats, incidents and solutions. See www.nlawarp.gov.uk.

Being a member of a regional WARP will also ensure the Security Manager is able to advise and keep the SIRO updated with current issues and best practice.

Places

All Local Public Services should ensure the security of their information through the physical security of their buildings, premises and systems. There should be regular assessments of physical risks to information, which are then discussed by senior management. Physical security should be layered so that the most important processes are undertaken in the most secure areas.

Undertake regular risk assessments

Local Public Services should undertake regular risk assessments to ensure the confidentiality, integrity, quality 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 and the Corporate Information Governance Group.

Information risks should appear on the corporate risk register; this is a resource for highlighting information risk being cross-organisation, and not just and ICT issue.

In addition, risks can be reduced by:

- Ensuring buildings and premises are secure. Issue all staff with ID cards - ensure that they are worn and challenge people that are not wearing them.
- Recording all visitors to buildings and, wherever feasible, ensure that they are accompanied whilst on the premises.
- Implementing 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.
- Ensuring rigorous adherence to all security policies (e.g. access control, password use, homeworking, data sharing, equipment disposal, BCM etc etc)
- Ensuring where personal information is held on paper, it is locked away when not in use or the premises are secured. Sensitive Paper files should be transported appropriately and securely.
- Ensuring the secure disposal of information, whether electronic or paper based. This requirement is a major source of data losses that have incurred a penalty or enforcement under the Data Protection Act (DPA).

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

Wherever possible avoid the use of removable media

Wherever possible Local Public Services should avoid the use of unencrypted removable media including laptops, removable discs, CDs, USB memory sticks, PDAs and smartphones. Where it is unavoidable, for personal information and other confidential files, **encryption must be used**. Those using smart phones and tablets must be aware of the risks involved**.** The information transferred to these devices should be the minimum necessary to achieve the business objective. (barest minimum = minimum)

Processes and systems

All Local Public Services should ensure that all processes, relating to systems operation and interfacing are properly documented with up to date information; such processes should be included in a risk assessment. It is essential that the SIRO and IAO, understand fully, where information is created, processed, stored and finally destroyed. Cloud services will highlight this problem further, where service assurance will be given through a robust accreditation process offered by the PSN. The service will be accredited once and used many times thereafter. This is explained in the PSN Security Model.

In addition, Local Public Services should ensure that:

- All systems containing personal information should have Privacy Impact Assessments carried out on them.
- The same controls apply for all third party provided systems; suppliers and contractors must be subject to the organisation's policies and procedures.
- They monitor and audit the effectiveness of their policies and, where appropriate, engage independent experts to test ICT systems and make recommendations.

Local Public Services should also:

- Work towards a policy of least privilege, wherever possible, access to systems should be restricted to only those users that need it.
- Limit access to raw data (containing personal information) so that it is strictly controlled and, where possible, only anonymous data should be readily available. For controlling access to systems, use of the cross-government Employee Authentication Service (through the PSN) is an option which should be considered.

A standards based approach to service management is recommended. The Information Technology Infrastructure Library (ITIL) contains a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. ITIL describes procedures, tasks and check lists that are non-organisation specific that can be used by an organisation for establishing a minimum level of competency. It also allows an organisation to establish a baseline from which it can plan, implement, and measure. It can be used to demonstrate compliance and to measure improvement. ISO 20000, is the certification standard, for ICT service management, it works in close conjunction with the ISO 27000 series of information security management standards, which are the baseline for the security assurance of PSN services.

Personal information should be kept within secure premises and systems

Local Public Services should take care to ensure that their information is transmitted, stored and processed on systems which offer adequate levels of assurance, security and protection for the information in use. All personal information is subject to the Data Protection Act and the subsequently the ICO issues civil penalties for failing to adequately protect personal information.

Whenever possible, the transmission and processing of personal information should be carried out using a trusted secure network. PSN, GCF(GSi, X.GSi, GSX, GCSx, GSE), N3 and PNN offer are examples of assured, trusted networks via which information could be accessed and transferred, depending on the impact level of the information. These networks also enable collaboration between Local Public Services and other public sector partners at reduced risk and greater efficiency.

Organisations should pay particular attention to the security of the systems on which their bulk and aggregated data is stored and the mechanisms used to access and transfer that data by users and business partners.

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 encrypted computer on a secure site on which it can 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. If removable media has to be used, and supported by a business case, the media must be encrypted.
- Wherever possible, the bulk transfer of information should only be carried out via a secure network.
- Where it is necessary to bulk transfer information, it should be done electronically across the secure network.

- Whenever possible, we strongly recommend two factor authentication be deployed for access control.
- Where information needs to be shared between public sector organisations, the Public Services Network (PSN) or GCSx (Government Connect) will be used wherever possible. This will facilitate the 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 – even when encryption is used. Properly designed and configured bulk file transfer services should be used.

Engage independent experts to carry out penetration testing

All Local Public Services should engage independent experts who are appropriately qualified members of TigerScheme, Crest, or CHECK to carry out penetration testing of all ICT systems where it is deemed necessary. The PSN, GCSx, N3 and other networks require annual network security health checks ('Penetration Testing'). These annual tests need to be carried out, reviewed and acted upon.

The scope of IT Health Checks must as a minimum include, websites, wireless networks, mobile devices, servers, network gateways and access controls. The scope of the IT Health Check and the report produced should clearly identify all vulnerabilities and make recommendations for mitigations and remedial actions. These should reference the code of connection controls the vulnerability relates to. IT Health Check reports should be easy to read and understand, to assist the SIRO in ensuring required remedial actions plan is carried out and completed during the current year.

The checks should also cover the Personnel and Physical security aspects of the corporate network and its controlled devices. In addition, the Code of connection requirements should ensure that all inter-connected third party networks are at least as secure as the main network. All networks are to be properly documented, and diagrammed, with a robust change control and patching regime in place.

Conduct Privacy Impact Assessments

Where appropriate conduct Privacy Impact Assessments (PIAs) for new systems being implemented. PIAs 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 (primarily data subjects) and a search is undertaken for ways to avoid or minimise privacy concerns….".

Full documentation and guidance materials to complete PIAs are freely available on the ICO website.

New ICT systems should be accredited to Government standards

For new systems containing personal information or other confidential information, Local Public Services should aim to have services accredited to Government standards, for use in a PSN environment.

Whilst formal accreditation for new systems in Local Government is not mandatory, there does need to be an understanding of the value and impact of information stored and processed in a system to ensure proper technical controls are applied to protect that information. (There is a requirement of the Data Protection Act (Principle 7) to ensure appropriate and adequate technical measures to safeguard personal information.)

When procuring new systems, Local Public Services 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. The PSN environment will through the PSN authentication service be able to help in this audit and monitoring process.

Ensure that your suppliers and contractors adopt equivalent standards

Local Public Services should mandate equivalent standards where they can and seek to influence others where they cannot mandate in all instances when suppliers and contractors are handling information on their behalf. There are contractual obligations in the Data Protection Act that require the contracting authority to be satisfied as to the standard of security offered by suppliers and contractors who process personal information, and to assess that those standards are maintained throughout the period of the contractual relationship.

Procedures

All Local Public Services 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 Local Public Services.

Produce a Corporate Information Risk Policy

The policy should set out how to implement the measures in this document in relation to Local Public Services 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, the SIRO, or a nominated individual on their behalf, should complete a Corporate Information Risk Plan. This plan should be reviewed through the Corporate Information Governance Group (CIGG). Review all assessments and examine forthcoming potential changes in services, technology and threats. This should form the basis of the Corporate Information Governance work plan for the following year.

Produce a Risk Recovery Policy

Local Public Services 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 Local Public Services' media and legal response, and should have clearly defined responsibilities. All staff should be made aware of this policy.

Local Public Services are urged to have an annual training and desktop exercise to test the effectiveness of these plans.

Risk reporting mechanisms

Serious Security incidents should initially be reported to the Regional Local Authority WARP. Serious network security incidents affecting either GCSx, GSX, GSi, PSN, N3 or PNN **MUST** be reported to GovCertUK.

For further details see www.nlawarp.gov.uk.

Significant, actual or potential losses of personal information should be notified to the Information Commissioner's Office (ICO) in accordance with ICO guidance; failure to do so could risk immediate enforcement action. The ICO will undertake free on-site data protection audits to varying levels of detail. The ICO has a free helpline that advises on all aspects of data protection compliance including responses to data loss incidents.

Regularly review, test monitor and audit all policies and procedures

Local Public Services should regularly review, test, monitor and audit their policies and procedures. This should include a range of measures from testing awareness and the 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 and destruction of information.

Information Sharing Protocol

The Information Commissioner has published a statutory Code of Practice on data sharing; failure to adhere to this guidance will become an important factor in any breach of procedure in connection with data sharing.

Sharing personal information about people is central to effective care and service provision across the whole service sector, both public and private. Several high profile national failures where organisations have not shared information (Climbie, Soham, etc) have highlighted this. It is generally recognised that sharing information can bring many benefits in providing integrated services and in safeguarding and promoting those services. In particular, it concerns those organisations that hold information about individuals and who may consider it appropriate or necessary to share that information with others. The ISP should provide a framework for staff to work with to identify what information they need to share, and should be sharing, with partner agencies and document agreed terms for that sharing.

An information sharing protocol should set out the purposes for sharing specific sets of information for a specific business purpose. It is aimed at operational management and staff, to provide them with details of:

- the processes for sharing information
- the specific purposes served
- the people it impacts upon
- the relevant legislation powers
- what information is to be shared and with whom
- where the information will be stored, processed and transmitted
- any operational procedures
- the process for review
- how and when the information will be destroyed
- how a breach will be notified and managed
- adherence with other recommendations in the statutory data sharing code of practice
- any consent process involved

Wales Accord for Sharing of Personal Information (WASPI) is a framework used in Wales for service providing organisations directly concerned with the wellbeing and safety of an individual, to share personal information between them in a lawful and intelligent way. It applies to all public sector organisations, voluntary sector organisations and those private organisations contracted to deliver relevant services to the public sector who provide services involving the health, education, crime prevention and social wellbeing of people in Wales. It is made up of two parts: the Accord and supporting Information Sharing Protocols. WASPI is an exemplar for Information Sharing Protocols.

The Accord is a common set of principles and standards under which partner organisations will share information. WASPI is part of the Sharing Personal Information (SPI) programme. The programme was established to enable public sector services, as well as third party and private sector providers, where appropriate, to share personal information on individuals; legally, safely and with confidence. Its aim is to ensure that the public receive services that are coherently and collaboratively delivered and effectively based on need, and safeguard the individual when necessary. In Wales, organisations need to jointly develop supporting information sharing protocols using the Guidance, template and check list provided on the WASPI website (http://www.waspi.org).

Appendices

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 and understands 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 (CIGG)
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.

Top Ten Tips for Mobile Devices

1. Understand and evaluate the risks of the use of such devices.
2. Have policies in place, which require contextual awareness training.
3. Each person signs a personal undertaking to protect the information on the device.
4. When staff leave, they should sign an undertaking Local Public Services data has been deleted from their personal devices.
5. All device security features should be enabled, firewall, password, pin and encryption.
6. Ensure the device is regularly patched / updated. Limit device features.
7. Ensure devices and corporate personal data is encrypted, use two factor Authentication wherever possible.
8. Use a shell/secure application environment on the device to protect corporate information.
9. Review the risks associated with the use of the at least device annually, or when a significant change occurs, if sooner.
10. Aftercare, ensure the ongoing delivery of updated information and training on device risks, including a Help Desk and incident reporting process.

Useful resources

The Information Commissioner's Office (ICO)

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

- The Information Commissioner’s Office Website is available at http://www.ico.gov.uk

WARP (Warning, Advice and Reporting Point)

Regional Local Authority WARPs are communities of practice delivering subscription based services where members meet face to face and share up-to-date advice on information security threats, incidents and solutions. The WARPs also support training and professional development for their members and undertake an annual risk survey, for benchmarking IA maturity.

- More information about WARPs in Local Government can be found at http://www.nlawarp.gov.uk

The National Technical Authority for Information Assurance, CESG

CESG as the National Technical Authority (NTA) protects and promotes 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.

- The CESG website can be found at http://www.cesg.gov.uk

UK Government Incident Response team (GovCertUK)

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.

- The GovCertUK website can be found at http://www.govcertuk.gov.uk

Local Government IA policy repository

This repository is maintained by the NLAWARP, as a common good initiative to provide local public services with some basic Information Assurance policy examples and other material to help them implement Information Assurance and Governance.

- This repository can be found at http://www.g3ctoolkit.net

National Archives SIRO Training

The National Archives, on behalf of the Office of Cyber Security and Information Assurance (OCSIA) in the Cabinet Office, is responsible for delivery of the Information Assurance training programme to public sector employees. Organisations covered by the Data Handling Review must demonstrate they have met the training requirements described in 'Data Handling Procedures in Government: Final Report June 2008'. Completion of this training programme will help to achieve this. National Archives also has information about records management and data quality.

- This SIRO Training material can be found on the National Archives Website at : http://www.nationalarchives.gov.uk/information-management/training/information-assurance-training.htm

Information Technology Infrastructure Library (ITIL)

The Information Technology Infrastructure Library contains a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. ITIL describes procedures, tasks and check lists that are non-organisation specific that can be used by an organisation for establishing a minimum level of competency. It also allows an organisation to establish a baseline from which it can plan, implement, and measure. It can be used to demonstrate compliance and to measure improvement.

- The official ITIL website can be found at: http://www.itil-officialsite.com

Wales Accord for Sharing of Personal Information (WASPI) http://www.waspi.org

A framework used in Wales for service providing organisations directly concerned with the wellbeing and safety of an individual, to share personal information between them in a lawful and intelligent way. It applies to all public sector organisations, voluntary sector organisations and those private organisations contracted to deliver relevant services to the public sector who provide services involving the health, education, crime prevention and social wellbeing of people.

- Further guidance on Intra NHS Information Sharing in Wales can be found at http://www.wales.nhs.uk/sites3/Documents/783/Intra%20NHS%20final1.doc.

CPNI (The Centre for the Protection of National Infrastructure)

CPNI provides integrated security advice (combining information, personnel and physical) to organisations which make up the national infrastructure. CPNI's advice helps to reduce the vulnerability of the national infrastructure (primarily the critical national infrastructure) to terrorism and other threats to national security.

- For more advice, see their website http://www.cpni.gov.uk

These guidelines were produced by the National Local Authority Warning, Advice and Reporting Point (NLAWARP) Programme, supported by the PSN team.

NLAWARP

Local Government Association

socitm
Local CIO Council

Cefnogir gan
Lywodraeth Cymru
Supported by
Welsh Government

Public Services Network
7th Floor, Aviation House
125 Kingsway
London
WC2B 6NH

© Crown copyright 2013

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit http://www.nationalarchives.gov.uk/doc/open-government-licence or email psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

Any enquiries regarding this publication should be sent to us at:
public-services-network@digital.cabinet-office.gov.uk