Local Public Services Data Handling Guidelines

Fifth Edition

April 2018

iStandUK

BRIDGING THE INFORMATION GAP

Acknowledgements

The NLAWARP team thanks those who have commented and continued to support this work, especially;

Helen Dolman Powys County Council
Sarah Gallear Warrington Borough Council
Chris Pounder Amberhawk Associates

Principal Author: **Mark Brett** Programme Director NLAWARP

mark.brett@nlawarp.net

Table of Contents

Foreword

Over the past twelve months since the previous edition of these guidelines were published much has happened, not least the change from a Data Protection regime based on Directive 95/46/EC to one based ono the General Data Protection Regulation (GDPR) and the WANNACRY attacks which affected many organisations globally. There have been changes to the Public Services Network (PSN), with the move to the PSN being a network with a baseline compliance regime, that does not provide any level of information assurance beyond it requiring a level of compliance.

The National Cyber Security Centre (NCSC), continues to provide technical and policy support to the Local Public Sector, but this support is dependent on strong information governance, supported by the Senior Information Risk Owner (SIRO) and Information Asset Owners (IAOs). There has to be a local information risk management regime in place, which supports a written information risk appetite for the organisation, managed and scrutinised by a Corporate Information Governance Group.

Organisations must have a robust training regime in place for all staff, contractors and suppliers, to ensure they know how to protect personal data. Organisations need a general awareness raising campaign to support GDPR and Cyber Resilience. Training records need to be kept in case there is a data breach to provide evidence to the ICO. Organisations must have a robust and well rehearsed Incident response capability in place, this needs to be fit for purpose to support GDPR breaches and Cyber Security incidents. The National Cyber Security Programme (NCSP), continues to provide valuable additional support and initiatives to enhance cyber security and capability in the UK.

Local Cyber Resilience and the protection of frontline government services is becoming a new priority area, this extends to securing local democracy through the protection of local and national elections. The recognition of cyber resilience as a focus area moving forward, along with the additional requirements for GDPR, should highlight the need for Local Public Services to plan, prepare and exercise for when things go wrong. This has always been a background requirement of the Civil Contingencies act, but as we move forward, those engaged in the work of the local resilience forums (LRFs), will start to focus on and plan for cyber incidents.

The regional WARPs provide a strong community of practice and a platform for shared learning, collaboration and knowledge sharing, fifteen years after their creation they are as relevant now as they ever were to help local public services prepare and respond to the ever emerging threat of cyber attacks. Organised crime continues to be the number one external threat to organisations, but the insider threat is still the number one cause of data breaches, though staff error and negligence, which can be largely addressed through training and awareness raising. We continue to improve as a sector, but still have much work to do. These guidelines help by providing a wide range of relevant information brought together into a common narrative.

Mark Brett

Programme Director NLAWARP April 2018

Background

Information continues to be the key business asset and is fundamental to the delivery of public services - are you doing enough to protect the data entrusted to your organisation? The UK Government has decided to include the obligations of controllers and processors identified in the GDPR as part of the Data Protection Act 2018. There have messages and assistance from the ICO coming out over the past two years to help organisations prepare. Even after May if GDPR preparations are not completed, it will be essential to have a published, tracked and monitored implementation plan and a register that contains details of all the organisation's processing activities , your required under GDPR A.30 to have a register of processing activities, (ROPA), with respect to personal data. If something untoward should happen, you will then have evidence of action in the form of your plan.

In further detail, that processing register must contain:

1. the name and contact details of the controller and, where applicable, the joint controller and any data protection officer;
2. the purposes of the processing;
3. a description of the categories of data subjects and of the categories of personal data;
4. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
5. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
6. where possible, the envisaged time limits for erasure of the different categories of data;
7.)where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

See: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

The reliance and use of cloud services have increased, applications such as Microsoft Office 365, is now becoming the preferred option in many organisations, this improves resilience as it removes the reliance around on premise email exchange servers, but needs to also have the active directory services to be cloud based as well. Directory services will be another increasing growth area, which will need digital certificates to back up and protect device encryption and access control.

The threat from cyber attack has increased. Bring your own device and remote connectivity have increased in popularity and availability and the Government has begun to implement a new protective marking scheme. The PSN (Public Services Network), has changed its emphasis from being and eco-system, to just focussing on just being a network.

See:https://www.researchgate.net/profile/Mark_Brett/publication/305800395_Public_Services_Network_Overview_Report/links/57a2074b08aeef8f311de425.pdf?origin=publication_list

Protecting personal data is a legal requirement under the Data Protection Act 2018/General Data Protection Regulation. The Act establishes a framework of rights and duties which are designed to safeguard personal data and balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details. [All references to GDPR will read Data Protection Act 2018 from May 2018].

The added complexity of off-shoring cloud services and the demise of international agreements such as Safe Harbour which allowed transfers to the USA (and possible issues with its replacement Privacy Shield), has also brought new challenges, requiring management decisions to be made.

The emphasis moving towards the Senior Information Risk Owners (SIROs) making and being accountable for local risk management decisions within their organisations and scope of authority. Although central government is moving away from the SIRO job title, the responsibility and function will remain. It is essential local public services keeps and maintains the SIRO function, at a senior level to ensure local information governance and leadership. Under the DPA/GDPR, public authorities must appoint a Data Protection Officer (DPO).

The DPO has certain minimum tasks that are defined within the DPA/GDPR and requires that they have professional knowledge and experience of data protection law (although no particular qualifications are specified). Organisations may therefore wish to consider whether the DPO will be the same person as the SIRO or whether this will be a separate role. There could be a conflict of interest between the SIRO and the DPO if the SIRO accepts a serious risk decision affecting personal data that a truly independent DPO would find unacceptable.. The DPO must be independent and can be shared by a number of organisations. The ICO has said they would expect all Local Authorities to have a DPO. For more info, see the ICO's online DPA/GDPR guidance on Accountability and Governance: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/

The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO will take action where appropriate to ensure compliance with the Act and now has a range of enforcement actions including the power to fine organisations up to £500,000.00 for non-compliance. Under the DPA/GDPR, the maximum penalties for non-compliance are set to rise significantly, with certain types of breach being subject to fines of up to 20 million euros.

The DPA/GDPR does provide that Member States should be able to determine the extent to which

these fines should apply to public authorities (or indeed whether they should apply at all). However there is at the very least the potential for significantly increased maximum penalties for public sector organisations. Trust needs to be maintained with citizens and business. Any processes implemented need to be proportionate to the information risk. Local Public Services will still face the full financial penalties for any breaches.

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.

The continuing high profile losses of data by public and private sector organisations reduces the confidence in the public sector. Many of the data losses are wholly preventable, being the result of failings in both technical and organisational measures also inappropriate disclosures.

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 not only trust that their privacy is protected and their personal data is handled professionally but that Local Public Services can provide appropriate assurance that it is. DPA/GDPR requires organisations to be able to demonstrate their compliance.

Back 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. The austerity agenda, (although coming to an end) has and will drive transformation and change towards shared services. The PSN compliance regime is based around commercial good practice. The compliance regime covers network technical controls. There is a need to focus on Information Governance and Risk Management.

The ever increasing sophistication of cyber attacks will continue, organisations need to be aware of issues relating to off-shoring data into cloud services, trying to ensure cloud data is kept within the EU. New Data Protection regulations from the EU, with the demise of the existing safe harbour agreements will further complicate the landscape, for data held in the US, there is now the privacy shield. It is critical that organisations carry out a Data Protection Impact Assessment on all personal data that is to be processed and stored outside of the EEA. Information outside of the EU and definitely outside of the EEA, MUST demonstrate a level of adequacy to provide sufficient confidence to the Data Controller and SIRO.

See: http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

Articles 40-49 of the GDPR as amended by Schedule 6 of the Data Protection Act 2018 covers the

law with respect to off-shoring.

See: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/

This new edition of the Local Public Services Guidance reflects those changes and highlights the progress made. We acknowledge that there has been progress. However, the number of monetary penalties issued by the ICO to local public service organisations clearly demonstrates that there is still some way to go. Whilst there haven't been many fines to Local Authorities under the Data Protection Act, the DPA/GDPR is likely to change this. Preparing for DPA/GDPR now, is the best mitigation. This document develops an approach to help organisations to move towards an Information Governance regime that is fit for purpose for a Local Public Services environment including Public Services Network (PSN). The guidance is equally valid for those organisations not directly connected to the PSN.

This document recognises that ***Local Public Services are best placed to assess their own risk and put in place the necessary safeguards***. This guidance aims to serve as a checklist, 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 PSN now has a much simplified compliance regime, which whilst making compliance simpler to attain, the bar has not been lowered and there is an element of trust that organisations will mitigate the risks they have identified to the PSN compliance team.

The Government's Security Policy Framework (SPF) is not mandated for Local Government, but it is relevant. This guidance also details the simplified Government Security Classification Scheme and Furthermore this (Data Handling) guidance outlines the roles and responsibilities of Local government SIROs (Senior Information Risk Owners) and IAO's (Information Asset Owners). Under DPA/GDPR all public bodies such as Local Authorities will require a Data Protection Officer to be appointed; however for smaller public bodies, there can be shared Data Protection Officers

Whilst not mandated on Local Authorities, the SPF (Security Policy Framework), is recommended and an integrated approach to risk management and Information governance. 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. Likewise the Cyber Essentials framework and the ten steps to Cyber Security are wholly recommended to organisations to follow, especially their supply chain suppliers.

Finally, the DPA/GDPR has specific security obligations that need to be evidenced. These are identified in Article 32:

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

    1. the pseudonymisation and encryption of personal data;

    2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

    3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

    4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

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. There are links provided later to specific ICO resources that contain the actual guidance and explanations. Likewise, there are links to NHS guidance that provides the actual requirements for Health organisations.

Secure data sharing is central to the success of all electronic information sharing within Local Public Services. This sharing, must be balanced and proportionate according to the business requirement, whilst preserving privacy and transparency whenever necessary, which could include data sharing with law enforcement. Data Controllers must consider how personal data can be kept safe and how it should be handled, rather than 'whether sharing of particular data in a particular way' is desirable. All processing, storage and sharing of personal data under DPA/GDPR requires a legal basis to do so.

Issues around whether personal data should be shared, still continues to be covered by regulatory, statutory and business driven risk decisions. The Information Commissioner's Data sharing code of practice (updated for the new data protection regime) provides a framework for making good

quality decisions about data sharing of personal data and includes a series of checklists designed to help organisations decide whether to share data, and what to consider when sharing it.

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 NCSC formally CESG (the Communications and Electronic Services Group, part of GCHQ). All connections to the PSN are based around the basic technical controls of ISO 27001. Remember PSN is only a network. PSN compliance is NOT a general security assurance certification; it just says your network is compliant, nothing more.

The technical controls are augmented with both Personnel and Physical Security requirements, provided by CPNI. This data handling guidance builds on those controls as specialist advice for Local Public Services and the voluntary sector. We are also seeing the emergence of the agile development methodology, to support digital products, which will help make citizen facing digital services simpler and more cost effective.

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 continues to be structured around five headings:

- People
- Places
- Policies
- 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 Local Public Service Organisations can be assured that steps were taken to prevent and mitigate such an occurrence.

The General Data Protection Regulation is underpinned by a set of principles and the key to complying with the DPA/GDPR is to follow the principles If you make sure you handle personal data in line with the principles you will go a long way towards ensuring you comply with the law.

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 a Useful Resources section which, covers offshoring, increasingly relevant for cloud computing.

People

All organisations should seek to develop a culture so that ALL staff (including your suppliers) 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. Some Local Public Services have explored "Bring Your Own Device to Work (BYOD)" or issuing staff with individual portable devices for data storage in the field and at home. BYOD specifically refers to consumer devices, which are not owned, managed or controlled by the organisation.

For ICO Guidance on BYOD see: https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

The use of Consumer type devices which are owned and managed by the organisation, is covered in the Government Digital Service End user Device Guidance, which is on the gov.uk public website. This guidance, covers a wide range of popular devices. In addition, specific context awareness training is essential. The organisation's boundary is no longer its buildings, it is now the mobile device.

See: https://www.ncsc.gov.uk/topics/byod

Appropriate staff vetting and background checks, should be carried out as 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 department responsible for advice relating to personnel and physical security. 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. Whilst it is no longer a mandatory requirement for PSN access to have staff vetted, organisations should understand the value of vetting and where it is appropriate.

The BPSS document is available at:

https://www.gov.uk/government/publications/government-baseline-personnel-security-standard

Personnel security is also a vital component of any information risk management regime. Insider threat is a credible and increasing attack vector, whether accidental or deliberate, through disgruntled staff, blackmail or through coercion. Organisations such as DWP, may still have specific vetting requirements to access their systems, aside from any PSN requirements. Again CPNI offer advice on their website. Most data breaches are caused through staff negligence, (insider threat). Training and awareness raising are the best line of defence to reduce this. Think before you click.

Governance roles and responsibilities

Ensure a Senior Manager fulfils the function of Senior Information Risk Owner (SIRO) to ensure there is accountability

The Public Services Network (PSN) compliance, 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 the Data Protection Officer, 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 Data Protection Manager needs to be independent with a reporting line to the SIRO and Chief Executive or senior director. Whilst the SIRO could be the DPO, it's not a good idea as there could be a conflict of interest. Each organisation will have to make their own decision.

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

See: http://www.nationalarchives.gov.uk/information-management/training/information-assurance-training/what-resources-are-available/

The NLAWARP can also provide SIRO advice training and support through the WARP network.

It is recommended the Council Information Security Manager, to be NCSC Certified (CCP). The local 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. There are three levels, Practitioner, Senior and Lead. The NLAWARP can offer support and training through the

WARP network. CCP is available through the IISP, BCS and AMP Group. The process is a portfolio based submission, with a profession interview at the Senior and Lead Level and an exam at the Practitioner entry level.

The Local Public Services organisation 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 are Business Managers who operationally own the information contained in their systems. Their role is 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.

It is a requirement of the DPA/GDPR that the Data Protection Officer is experienced; this infers that some specialist training of the Data Protection Officer may be required.

Identify Users and their access rights

As 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, audited and pro-actively managed. All of these aspects form part of an information risk management regime.

Users (in the context of 'personal data' are those staff, contractors and suppliers who access and process any information (e.g. 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 needs to be reviewed and revoked where necessary.

Looking to the future, the data minimisation principle and data protection by design functionality in the software will help ensure that staff only gain access to the personal data they need to perform their functions.

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. The ICO may expect to see these records, should a breach be notified.
- 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 In some circumstances, breach reporting will be required under DPA/GDPR within a time limit. Incidents that pose a "high risk" to data subjects will need to also be reported to data subjects directly. For more information, please see the ICO guidance on breach notification under GDPR.
- 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. 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 SIRO, Corporate Information Governance Group (CIGG) and 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. Look at the ICO Data SharingCode of Practice

Efficient and effective use of personal data processed by public bodies is a good catalyst for driving transformation and efficiency; however such uses must demonstrate that they have complied with data protection law

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 central and local public service websites.

The ICO's DPA/GDPR guidance on accountability should be followed. In particular, it is stressed it is the controller's responsibility to "implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation" (see Article 23).

.

Sources of help and assistance

The National Archives publish various support guidance and documents to help SIROs . All SIROs are urged to register with the National Archives. The regional WARPs supported by the NLAWARP, also provide SIRO support, through the WARP members.

The CISP (Cyber Industry Security Partnership), is a free to join collaboration portal available to all Local Public Service organisations at https://www.ncsc.gov.uk we urge all organisations to join CISP. The CISP is not a substitution for a WARP. The WARP provides much needed face to face contact, training and briefings.

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.net

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.

The LGA and Welsh LGA are committed to supporting better information Governance and Management, through the LGA Local Government PSN Board.

Information Assurance continues to be a priority issue for the Local Public Services CIO Council and the Local Government PSN Board.

Cyber resilience is now a key priority and is regularly discussed at these governance boards. The work of the boards is disseminated out through the regional warps.

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, resilience, 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 and the Corporate Information Governance Group. The quality of all stored information forms an important part of information integrity.

Information risks should appear on the corporate risk register; this is a resource for highlighting information risk being cross-organisation, and not just an 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 staff have the confidence to challenge people that are not wearing them.
- Recording all visitors to buildings and, wherever feasible, ensure that they are accompanied whilst on the premises.
- Including your physical security requirements in all supplier contracts.
- 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, Business Continuity Management etc)
- Where cloud services are being used, it is essential the personal data is stored within the EU or other recognised domain, Utilising the ICO model contract Clauses.

  See: http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing
- Cloud Security principals should be followed.
- Cloud services require their own Business Continuity Plans and approach.
  Many data breaches relate to printed records, letters and faxes etc.
- Ensure you have business continuity plans in place. Carry out an annual exercise.
- Ensuring where personal data 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.

- All personal data 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. The CESG Product Assurance Scheme(CPA) will help with this.

See also http://www.cpni.gov.uk/advice/Physical-security/secure-destruction-of-sensitive-items/

Wherever possible avoid the use of removable media

Where personal data is involved, Local Public Services must avoid the use of unencrypted portable media including laptops, removable discs, CDs, USB memory sticks, PDAs and smartphones, where personal data is being stored. Failure to do so would almost certainly be a reportable data breach under the Data Protection Act, which is likely to result in formal enforcement action being taken. There needs to be a practical and pragmatic approach to this issue.

The widespread introduction or cloud services now negates the need for USB devices for data transfer. The use of secure cloud transfer services should be considered. All cloud solutions should be enterprise editions of the service, to facilitate proper audit controls and encryption.

There are CPA approved file transfer and sharing cloud services available. Many leading email providers now provide cloud drives, which make file sharing simple, secure and controllable. File sharing should be monitored and auditable. Services like Google apps and Office 365, provide shared file storage. It is for the SIRO to determine whether the level of assurance provided, provides sufficient confidence. This includes taking account of the organisations risk appetite and Information Governance regime. Any Government information, will be subject to off-shoring guidance and constraints.

Always seek assurances about where cloud data is stored. This is your local responsibility. Check G-Cloud assurances and accreditations. Where it is unavoidable, for personal data and other confidential files, **encryption must be used for data in transit and at rest**. Those using smartphones 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). All personal data stored in the cloud must be encrypted by default. This equally applies to processing, storage at rest and archiving.

Policy

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

Local Public Services should implement a range of security policies, to ensure compliance with the PSN and HSCN regimes. An example selection of policies are available on the NLAWARP website www.nlawarp.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
- Business continuity and Cyber Resilience
- DPA/GDPR Breach notification and incident management and response.
- E-mail usage
- E-Mail protection, configuration and testing
- DNS Protection, configuration and testing
- Use & control of portable media
- Home & mobile working
- Secure document printing
- Manual (paper) document handling
- Handling of faxes
- Secure disposal and destruction of Information Assets
- Log Collection, processing, storage and management and analysis
- Disclosure of information by telephone, face to face and in writing.
- Information asset valuation
- Risk management regime
- Protective marking
- Use and control of personal devices
- Network, System and Device Configuration and Management
- The use and control of encryption software
- Forensic readiness
- Cyber Incident response, reporting and management

- Network Protective Monitoring and Situational Awareness
- Management control and monitoring of wireless networks
- Management, control and monitoring of web services
- Intrusion detection and monitoring
- System Access Control
- Patching systems, devices and network equipment
- Configuration management and change control
- Cyber Resilience and Business Continuity Management

It is essential that as the complexity and volume of threats increases, that the 5 core areas of Network Security are addressed;

- Boundary devices / Firewalls
- Access Control
- Patch Management
- Secure Configuration
- Malware Protection

  Whilst the issue around boundary protection is addressed, it should be especially noted that most attacks occur either through email payloads or through website attacks. Specialist attacks are aimed at applications and through the exploitation of vulnerabilities in software, exposed through poor patching. Patching continues to remain the single biggest defence against attack.

  These 5 areas are covered in the Cyber Essentials Scheme. Although Cyber Essentials has been developed for SMEs and other businesses, we believe it provides a simple and effective framework, which will help Shared Services, SME suppliers to Local Public Services and the Third Sector.

  In addition to the basic Cyber Essentials, there is also a more robust IASME standard, which includes full Cyber Essentials certification and additional risk and governance issues see: https://www.iasme.co.uk/

Processes

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 assurance process. 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:

1. All systems containing personal data should have Data Protection Impact Assessments carried out on them. The ICO recommends this and guidance is available in the ICO's Conducting Data Protection Impact Assessments code of practice. DPIAs (which are also known as Privacy Impact Assessments privacy impact assessments (PIAs)), should be an integral part of all project management processes and development, including agile. **Under DPA/GDPR, DPIAs will be mandatory whenever the processing** is likely to result in a high risk to the rights and freedoms of individuals. For example when there is:

    1. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

    2. processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

    3. a systematic monitoring of a publicly accessible area on a large scale.

See: http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment

- The same controls apply for all third party provided systems; suppliers and contractors must be subject to the organisation's policies and procedures. These arrangements should be formalised in contracts. Cyber Essentials / IASME can help.
- Looking forward, under DPA/GDPR, processors will also have their own legal responsibilities and can themselves be liable for enforcement action. Both Cyber Essentials and IASME have optional DPA/GDPR top-up compliance available.
- 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. Sharing the minimum information for a transaction or the least viable functionality for a software product, will enhance security.

- Limit access to raw data (containing personal data) so that it is strictly controlled and, where possible, only anonymous data should be readily available. Encryption of information and databases should be enabled by default, especially on cloud services. Controlling access to systems, using an approved Authentication Service should be considered. Any decisions on why encryption in transit, at rest was not implemented should be recorded.
- Use all of the available security options for cloud services. (Encryption of storage and databases).
- All data should be routinely encrypted, especially where cloud services are in use and when using portable media.

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.

ITIL 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 standards, which are the baseline for PSN services.

Agile Development

We acknowledge an increase in the use and deployment of agile developed products and services, this is fine and appropriate at OFFICIAL, we strongly endorse the GDS Service Manual and the NCSC Cyber Risk Principles. Where agile is being used, it is essential the information risks are fully understood and iterated at each release. Agile is not a reason to ignore Information Assurance. Anti-Personas and other techniques can be used at all staged of development. There is a wide range of supporting guidance in the GDS Blogs on gov.uk. Data Protection Impact Assessments can help with this. The DPIA can be an ongoing processes that is updated as necessary (rather than having to conduct a new DPIA each time) and, as mentioned above, can be built into an organisations normal risk assessment and change management processes

The Cyber Essentials scheme can help your suppliers achieve a level of compliance, to bring confidence that their organisations take Information Assurance seriously. Details on the .gov.uk website.

See: https://www.cyberessentials.ncsc.gov.uk

Personal data 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 data is subject to the Data Protection Act; the ICO can issue civil penalties for failing to adequately protect personal data.

It is essential from the SIRO down through IAOs that all staff are trained on protecting information. This training needs to be refreshed annually and detailed training records need to be maintained. If there is a data breach, the ICO may expect to see training records. As mentioned above, public authorities will be required to appoint a DPO under DPA/GDPR, who must have appropriate knowledge and experience of data protection.

Being able demonstrate adequacy of staff training will also be part of the DPA/GDPR's requirements to demonstrate compliance

You will need to maintain records and keep evidence. The ICO

The ICO will expect to see evidence in the event of a breach or incident and if this is in place, it could help reduce the potential of a fine or size of fine under the GDPR and Data Protection Bill

Whenever possible, the transmission and processing of personal data, should be carried out using, a trusted secure network. The PSN and PNN offer are assured at the network layer, via which information should be accessed and transferred.

There are a number of major providers for PSN connectivity, which offers a choice and variety in the market place. Whilst the NHS digital network is an untrusted network, there are ways to ensure the safe transit of information using encryption and other technologies. Organisations still need to assure themselves that any assertions made by PSN providers are valid, robust and fit for purpose. A supplier simply being on the PSN or G-Cloud is not itself sufficient assurance at OFFICIAL.

These networks are a step towards 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. Assurances should be sought from providers about their security processes and posture.

Where it is not possible to access information on secure premises and systems, the following 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, using VPN and encrypted transfer methods.
- Whenever possible, we strongly recommend two factor authentication be deployed for access control, whether at the system level or on access devices.
- Where information needs to be shared between public sector organisations, the Public Services Network (PSN) will be used wherever possible. This will facilitate the transfer of information across the wider PSN and interlinks with other secure Government Networks including Health and Criminal Justice. Encryption should be used with VPN links. Assurance across the connection should be sought.
    - Where cloud services are being used, it is essential the personal data is stored within the EU or other recognised domain. See: http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing
    - Cloud Security principles should be followed.
    - Where personal data is being processed outside the EU where there is not considered to be adequate, the ICO model contract Clauses. Another country considered to offer an "adequate" level of protection by the European Commission, then there would be no need for model clauses (although there would also be nothing stopping organisations from using them as long as they were appropriate for the contract in question).
    - Model clauses are intended to cover situations where personal data is being transferred outside the EU to a non-adequate country.

It is never acceptable to transfer bulk ***personal data*** via normal email services – even when encryption is used. Properly designed and configured bulk file transfer services should be used.

There are now approved G-Cloud assured services that can facilitate secure file transfer. Some of these services in addition to G-Cloud are also CPA approved. Always seek assurances about the type and level of assurance or accreditation a product or service offered.

Get written assurances about where the information is stored and processed. Ask to see the assurance certificate and residual risk statement. Although the product may be assured, it does not mean it is automatically fit for purpose for your organisations needs or requirements.

Your SIRO will need to agree the application is applicable to your organisation and within your organisations risk appetite.

Engage independent experts to carry out penetration testing

All Local Public Services should engage independent experts who are appropriately qualified members of Crest, or CHECK The NCSC penetration testing certification scheme. to carry out penetration testing of all ICT systems where it is deemed necessary. The PSN, PNN, Health and other networks require annual network security health checks ('Penetration Testing'). These annual tests need to be carried out, reviewed and acted upon. We strongly recommend always using a CHECK based, fully credentialed IT Health Check for PSN connected services. This ensures the correct scoping of the test and will give you the confidence the CHECK team is testing your network and systems against the latest threats. Any organisation processing personal data (including charities), should undertake appropriate testing.

The scope of IT Health Checks must as a minimum include;

- Web Services, including Websites
- Wireless networks,
- e-mail services,
- Cloud services
- DNS Services,
- Email security
- Mobile devices,
- Servers
- VPN Servers / Proxy Servers
- Network gateways
- Access controls systems
- Active Directory, Directory Services

Because of the prevalence of malware and cyber attacks, credentialed internal tests should also be carried out, that is full white box testing.

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 the required remedial action plan is carried out and completed during the current year. The detailed relevant and consistent reporting is another reason why we strongly recommend specifying a CHECK based IT Health Check. It is possible for a CHECK

company to undertake an IT Health Check outside of the CHECK scheme, which is why you need to be specific.

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.

Network Service Configuration

Since the last edition, much has changed with the sheer volume and complexity of cyber attacks. We are now recommending that e-mail and DNS services be reviewed and secured. The demise of the GCSx email system, give flexibility and freedom to source or build your own email services or to continue using the GCF service while the contract extensions last. It must however be noted that the GCSx email suffix can be retained even when moved away from GCF email services.

Secure e-mail Services

Email needs to be securely deployed. Follow the secure email guidance. TLS should be deployed in a secure and well configured way, Including DMARC, DKIM, SPF. Likewise, your email services should now be pen tested as part of the IT Health Check. There is guidance around TLS, its configuration, testing and deployment.

See: https://www.local.gov.uk/understanding-secure-email-guidance

IP Reputation

It is vitally important that IP Reputation is taken into account. The GDS network principles now recommend that IP addresses for e-services are published, through authoritative DNS services.

DNS Services

We recommend that DNS services be securely implemented and regularly scanned and checked. DNS Services should be part of the IT Health Check moving forward. The use of NCSC DNS service is recommended.

See: https://www.ncsc.gov.uk/blog-post/protective-dns-service-public-sector-now-live

Conduct Data Protection Impact Assessments

Conducting Data Protection Impact Assessments for new systems, should be one of the first considerations. This applies to new systems being implemented or old ones that are being updated. Data Protection 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 (primarily data subjects) and a search is undertaken for ways to avoid or minimise privacy concerns….".

Full documentation and guidance materials to complete Data Protection Impact Assessments are freely available on the ICO website.

See: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

New ICT systems should be assured to Government standards

For new systems containing personal data or other confidential information, Local Public Services should aim to have services accredited to Government standards, for use in a PSN environment. Whilst formal assurance 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. Ensure appropriate and adequate technical measures to safeguard personal data). There is also a requirement to have organisational structures in place, covering Information Governance, Technical Controls and Information Sharing Agreements.

All of these aspects need to be within a Risk Management framework. This is why both the legal requirements of the Data Protection Act and to some extent the PSN and IG Toolkit appear to cover the same ground. Only an organisation wide strategic approach will be effective to thoroughly protect information. NHS Digital has established a network for IG Managers.

When procuring new systems, Local Public Services should also consider putting in place arrangements to log activity of users in respect of protected personal data and for asset owners to check it is being properly conducted.

Ensure that your suppliers and contractors adopt equivalent standards

Local Public Service organisations should mandate equivalent standards where they can and seek to influence others where they cannot mandate in all instances when suppliers 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 who process personal data, and to assess that those standards are maintained throughout the period of the contractual relationship. Guidance on the controller processor relationship can be found at: https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf….

The data processor must provide sufficient guarantees in respect of the technical and organisational measures they take to protect personal data, and the data controller (in this paragraph the contracting authority) must take reasonable steps to ensure compliance with those measures. There must be a contract (in writing) which requires the data processor to act only on the instructions of the data controller.

Procedures

All Local Public Services should work towards producing 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.

Cyber Resilience

With the rise of cyber attacks and the increased sophistication of them, organisations need to prepare for cyber attacks. The "Think Cyber Think Resilience" work implemented by MHCLG under the Nation Cyber Security Programme can help.

A good starting point is the strategy report produced as part of the programme:

See: http://www.stgeorgeshouse.org/wp-content/uploads/2016/04/Local-Leadership-in-Cyber-Society-Report.pdf

There are a lot of additional useful resources at:

http://istanduk.org/cyber-resilience/

The Emergency Planning College (EPC) can also help with specialist advice and guidance:

See: http://www.epcresilience.com

A brief note for charities

The NCSC have published specific guidance for smaller charities. There is also a threat assessment by the NCSC for charities.

Produce an Information 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. This plan will need to be updated to include any cloud services that may be deployed. The cloud service provider will not generally provide business continuity services as part of their core offering. Seek assurances of what and how they provide resilience. 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. Cyber Resilience will grow in importance moving forward. Local Public Services are urged to have an annual training and desktop exercise to test the effectiveness of these plans. These plans should cover Cyber Resilience including Cloud Services. Incident Management processes should also be tested.

Risk reporting mechanisms

Serious Security incidents should initially be reported to the NCSC. Organisations with a SIRO should also ensure the SIRO is informed as soon as possible. The DPO (Data Protection Officer) should also be informed if organisation has one. Under DPA/GDPR, public sector controllers must have a DPO and the DPO must be informed. If significant, actual or potential losses of personal data should be notified to the Information Commissioner's Office who would not look favourably on failure to report a serious breach. The Information Commissioner's Office will undertake free on-site data protection audits or information risk reviews to varying levels of mutually agreed detail. The ICO also has a free helpline that advises on all aspects of data protection compliance including responses to data loss incidents. There is ICO guidance that can help:
https://ico.org.uk/media/1562/guidance_on_data_security_breach_management.pdf

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. Consider the implications for cloud and mobile service. Also what would happen if email was lost or your website was unavailable?

Data Sharing Agreement

The Information Commissioner has published a statutory Code of Practice on data sharing which is available on the ICO website; failure to adhere to this guidance will become an important factor in any breach of procedure in connection with data sharing. Chapter 14 of the Data Sharing Code of Practice covers this in detail.

See: http://ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

Sharing personal data 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 many news stories 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.

These threats continue to emerge and the same mistakes continue to be repeated. Child Protection remains a critical issue. CEOP (Child Exploitation Online Protection), can provide help and guidance. CEOP is now part of the National Crime Agency (www.nca.gov.uk).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.

See: https://www.thinkuknow.co.uk

The Data Sharing Agreement 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.

A Data Sharing Agreement, 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
- Where and how long the information will be kept for.
- How the data will be destroyed and all parties informed.
- If a party of the agreement is succeeded or disbanded, what will happen to any information held.

The Wales Accord for Sharing of Personal Information (WASPI) is a framework used in Wales for service providing organisations directly concerned with the well being and safety of an individual, to share personal data 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 data 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 checklist provided on the WASPI website.

http://www.waspi.org/

Appendices

NLAWARP DPA/GDPR Top 10 Tips

1) Train your staff, raise awareness and keep records of all training carried out.
2) Appoint a Data Protection Officer – You can share one, you do need one.
3) Oversee DPA/GDPR implementation – Corporate Governance Group - have a plan.
4) Ensure supplier contracts protect your personal data - are they adequate?
5) Know where all of your personal data resides. Produce an information asset register.
6) Record Data Protection Impact Assessments for all systems. Manual and electronic.
7) Manage all devices whether corporate or personal, that process your personal data.
8) Maintain records and evidence of all DPA/GDPR related contracts and activities.
9) Be clear about all off-shoring decisions – where is the data is protection adequate?
10) Implement and exercise incident plans. Breach management and notifications.

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 that Local Public Services data has been deleted from their personal devices and have a full leavers policy in place
5. All device security features should be enabled, firewall, password, pin and encryption.
6. The device should be 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

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.org.uk***

DPA/GDPR breach notification: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/

WARP (Warning, Advice and Reporting Point) www.nlawarp.net

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.

The National Cyber Security Centre NCSC

The National Cyber Security Centre (NCSC) is the UK's authority on cyber security. We are a part of GCHQ. The NCSC brings together and replaces CESG (the information security arm of GCHQ), the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI).

The NCSC website can be found at *http://www.ncsc.gov.uk*

Wales Accord for Sharing of Personal data (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 data 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.


NLAWARP


Local
Government
Association
CLILC • WLGA
solace


CFOA
Chief Fire Officers
Association
CSF
Charities Security Forum
socitm
local CIO council


iNetwork
involve influence inspire