Identity Management and Privacy Principles

Privacy and Public Confidence in Scottish Public Services

The Scottish Government

OCTOBER 2014

Version 2.0

Contents

Ministerial Foreword

The Scottish Government wishes to drive forward trustworthy uses of data for public benefit. This is key to our focus on prevention in delivery of public services. Increasingly we will be using digital technology to support the wider design and delivery of services. Our strategy, shared with the wider public sector, " Scotland's Digital Future: delivery of Public Services" therefore sets effective management of data as a key theme. To secure public support it is vital that we maintain and enhance Scotland's reputation for the safe, secure and transparent use of data, as set out in our Data Vision for Scotland[1]. These *Identity Management and Privacy Principles* have been updated to support that Vision and its accompanying Action Plan.

These updated Principles refer to the most recent good practice codes and guidance, as well as including a new section: *Data use for Research and Statistics*. This reflects the increasing importance of data in the production of research and statistics which support informed policy making, operational planning, and efficient use of resources.

These Principles form a 'living document' and will continue to be reviewed periodically. I seek your support in adhering to the Principles and in disseminating them further.

John Swinney
Cabinet Secretary for Finance and Sustainable Growth
October 2014

[1] A Data Vision for Scotland http://www.scotland.gov.uk/Topics/Economy/digital/digitalservices/datamanagement/dmbvfs/dmbvfspdf

Information Commissioners’ Statement

As Information Commissioners, responsible for, respectively, the Data Protection Act and the Freedom of Information (Scotland) Act, we have a common interest in promoting information rights and transparency in the public sector. As such, we welcome the opportunity to contribute a foreword to the Scottish Government’s Identity Management and Privacy Principles. These principles were recently extended to consider the handling of data within a research environment and we commend this updated guidance for what is a rapidly changing data environment.

All organisations handling personal information have a duty under the Data Protection Act to ensure that they handle data fairly, lawfully and securely. Scottish public authorities are also committed to sharing data and information actively and appropriately to support openness, transparency and the delivery of more effective public services. Data protection should not be seen as a barrier to sharing information, including for research, if it is in the clear public interest to do so and due consideration has been given to the privacy dimension. Data protection, when properly applied is a helpful tool which promotes the safe and efficient handling of personal data for organisational or public need while respecting individual rights.

These Identity Management and Privacy Principles complement the legislation and offer positive steps which, if followed, will reduce the risk of inappropriate disclosure or loss.

Good data handling will help Scottish public authorities to build the trust and confidence of their citizens and clients, especially when supported by clear information about how the data will be used and reused .

These Principles won’t just encourage openness and transparency to the benefit of the citizen, but, applied properly, will lead to better public administration and more efficient service delivery, and also demonstrate respect for clients. We urge all Scottish public authorities to adopt them as a minimum standard in their handling of personal information.

CHRISTOPHER GRAHAM, Information Commissioner
ROSEMARY AGNEW, Scottish Information Commissioner

ico.
Information Commissioner’s Office

Scottish Information
Commissioner

Introduction

As described in our Data Management Board's Vision[2], data is being produced at phenomenal rates. And people are often asked by public service organisations to prove that they are who they say they are - either to prevent fraud or to show that they are entitled to receive a particular service or benefit, for example, free bus travel. Scotland needs to make sure it is managing and using data in a responsible way to benefit all aspects of society: safe, secure and easy online access to services to individuals; supporting more efficient delivery of services; analysis and research to support policy making, planning and decision making; and making data available to support economic growth.

People want to know that public authorities and other organisations respect their privacy and recognise the harm which may be done if personal information is collected or held unnecessarily, or lost or misused. These Principles have therefore been developed by the Scottish Government for policy makers and practitioners in public service organisations, to help ensure that respect for privacy is central to the way public services use data, and prove identity or entitlement. They will also help public service organisations to comply with data protection and human rights legislation. That legislation governs personal information management by providing privacy protection. These Principles do not impose a requirement on public bodies to introduce policies that go beyond legal requirements. However, they will enable public organisations to build on these requirements and to achieve best practice.

The Principles have been developed to give guidance on identity management[3] and privacy to public service organisations and they apply to all new systems and any systems which are being redesigned or redeveloped which involve identity management.

The Principles which follow cover the following six sub topics:

1. Proving Identity and Entitlement
2. Governance and Accountability
3. Risk Management
4. Data and Data Sharing
5. Data use for Research and statistics
6. Education and Engagement.

A Glossary and a Link to pages to contain examples, case studies and links to helpful resources is provided at the end.

These Principles form a living document

Updated versions will be issued when necessary, for example when legislation is changed; new legislation is enacted; or ICO guidance is updated or published. Whilst best endeavours will be made to update these principles, it will still be up to organisations to ensure they are complying with current law. You should always check www.scotland.gov.uk/privacyprinciples for the current version of these Principles.

[2] A Data Vision for Scotland http://www.scotland.gov.uk/Topics/Economy/digital/digitalservices/datamanagement/dmbvfs/dmbvfspdf

[3] The enrolment and subsequent verification that gives individuals trusted means to prove who they are to others and / or entitlement to a service or benefit.

1. Proving Identity or Entitlement

Only identify when necessary

1.1 People should not be asked to prove who they are unless it is necessary. A person making a general enquiry about a service should not need to provide any identifying information.

Ask for as little information as possible

1.2 People should be provided with an effective way of proving their identity or demonstrating entitlement to a service, based on the minimum level of information necessary. Therefore, public service organisations must only ask for the proof they need in order to establish entitlement to a service. For example, if all that is needed is proof that a person is retired, or over 18 years old, then no more proof should be asked for.

Identify only once

1.3 For services which are used frequently and for which identification is needed, public service organisations should give people a simple way to register once. Thereafter, unless there is a statutory requirement to prove identity, in many cases a person should be able to access the service by authenticating themselves using a token, such as a bus pass or library card that proves their entitlement without revealing unnecessary personal information. In other circumstances, a user name and a password or elements of a password may be required.

Identify your organisation too

1.4 Public service organisations must provide ways for people to confirm that anyone claiming to represent the organisation, whether in person, by telephone, in writing or online, does in fact do so.

Ensure that authentication is effective and sufficiently reliable

1.5 The authentication methods selected (in the context of 1.3) should take into account convenience to the individual and respect for the individual's privacy. Organisations should also ensure that the means of checking identity are sufficiently reliable. In particular, they should take account of the extent to which the mechanism generates false rejections and acceptances and the consequences of these, including potential prevention of access to services or benefits, or failure to prevent fraud. Public service organisations must not rely, as the sole means of authentication, on personal information such as mother's maiden name which is quite easily found out, as this may increase the risks of fraud.

Avoid discrimination

1.6 Organisations must take steps to ensure that people are not discriminated against unfairly (for example, on grounds of disability, age or ethnicity) or socially excluded as a result of the approach to identification or authentication.

Offer choice

1.7 As far as possible, people should be offered alternative ways to prove identity and / or entitlement.

2. Governance and Accountability

Adopt privacy and security policies & procedures

2.1 Public service organisations (see glossary) using personal information directly or on behalf of public authorities should adopt clear, coherent and verifiable policies on privacy and security. This should include policies which will aim to ensure that:

a) a Privacy Impact Assessment (PIA) or proportionate equivalent is conducted and published prior to the implementation of a project which involves the collection of personal information;

b) only the minimum amount of personal information needed for a specific purpose is collected, used or kept; that appropriate consent is obtained where necessary and that systems used for personal data comply with legal and regulatory requirements;

c) the best available, most cost-effective techniques that are appropriate to the organisation and function[4] are used to ensure the security of personal information throughout its lifecycle (including while organisations share information right through to archiving it). These must take into account factors such as legislative requirements and ICO guidance. In particular, the organisation must abide by government standards for the use of encryption for the storage and transmission of this information; and that staff follow relevant guidance issued by the Information Commissioner's Office (ICO)[5][6][7] and implement recommendations arising from the 2008 Scottish Government *Data Handling in Government* report;[8]

d) personal data is only retained as long as is necessary[9] and subsequently destroyed in a secure manner.

2.2 Public service organisations must ensure that the policies and standards are supported by appropriate procedures, control the use of authorisation and identity management systems and can deal effectively with compliance failures and breaches.

2.3 Responsibility and accountability for privacy should be assigned to a named senior management officer who reports to the Board or equivalent[10].

[4] ICO's The Privacy Dividend http://ico.org.uk/news/current_topics/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_DIVIDEND.ashx

[5] The ICO is the UK's independent authority set up to promote access to official information and to protect personal information by promoting good practice, ruling on eligible complaints, providing information to individuals and organisations and taking appropriate action when the law is broken.

[6] One related resource on the ICO's website: New approaches to identity management and privacy December 2007 http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/EDENTITY_HP_IDM_PAPER_FOR_WEB.ashx

[7] Data sharing code of practice http://ico.org.uk/for_organisations/data_protection

[8] 2008 Scottish Government Data Handling in Government report (www.scotland.gov.uk/Resource/Doc/229747/0062215.pdf)

[9] The Guide to Data Protection (http://ico.org.uk/~/media/documents/library/Data_Protection/Practical_application/the_guide_to_data_protection.ashx)

[10] HMG Security Policy Framework (www.cabinetoffice.gov.uk/media/207318/hmg_security_policy.pdf)

Audit

2.4 Public service organisations must take appropriate steps to be able to demonstrate that personal information can only be accessed by staff who are authorised to access the information as part of their legitimate job role. Organisations must ensure that they keep records of access to personal information, that there are alerts which prevent or identify inappropriate access and that access logs and alerts are reviewed regularly. This should not impact adversely on analytical studies, such as epidemiological research, for which guidance is available[11].

2.5 If a person discloses personal information to prove identity or entitlement, public service organisations should not take or retain copies of that information (such as scans of driving licences or utility bills) unless this is essential for legal or audit purposes. In such cases, it would not normally be necessary to retain a copy of the full document; only the minimum amount of information to fulfil the legal / audit purposes would be required.

Accompany personal information with metadata

2.6 Where personal information is collected or stored, all reasonable steps should be taken to make sure that it is accompanied by information about the source, consent notice, permitted uses, retention period and other relevant metadata (i.e. data about data). Where information is shared within or beyond the public authority, it should be accompanied by this metadata to facilitate proper management of the information at its destination.

Facilitate oversight and reporting

2.7 The Scottish Government should work with the ICO to facilitate spot checks and the use of the ICO's forthcoming inspection powers and should co-operate with existing oversight organisations to include privacy issues in their inspections and reporting.

Apply Principles to contracts

2.8 Where public services are provided by non public sector the contract must impose appropriate obligations on the private or third sector body.[12] In particular, where a public body has a contract with the private sector or the third sector, the contractor must be contractually bound to adhere to best practice as outlined in these Principles and other guidance. Public service organisations should ensure by contract that such organisations are required to permit the ICO to undertake spot checks on the processing of personal data being carried out in relation to the delivery of public services.

Parliamentary scrutiny of privacy impacts by lead committees

2.9 Where new primary or subordinate legislation is proposed, Scottish Government officials should consider whether privacy issues will arise. If so, an appropriate Privacy Impact Assessment should be undertaken and a summary of

[11] Data Sharing for Statistical Purposes: A Practitioners' Guide to the Legal Framework' at http://www.ons.gov.uk/ons/guide-method/best-practice/gss-best-practice/data-sharing-for-statistical-purposes/index.html

[12] Data controllers remain responsible for ensuring their processing complies with the Act, whether they do it in-house or engage a data processor.

impacts should be submitted for consideration by the lead committee in the Scottish Parliament.

3. Risk Management

Carrying out Privacy Impact Assessments (PIAs)[13]

3.1 Public service organisations must carry out an appropriate level of PIA for any new initiative that enables access to services and involves the collection, storage or use of personal information. Public service organisations must also carry out an appropriate level of a PIA if they are changing existing systems in ways which involve collection, storage or use of personal information.

3.2 Public service organisations should seek early involvement, at the policy development stage, of the ICO in Scotland.

3.3 Public service organisations must make PIA documents publicly available[14], with easy access, before a new initiative is implemented.

Auditing existing initiatives

3.4 Public service organisations should consider privacy and data protection audits for existing initiatives.[15]

4. Data and Data Sharing[16]

Acquiring and holding personal information

4.1 Public service organisations must minimise the personal information they hold, only acquire personal information for which they have a defined and specific need and ensure that such personal information is held only as long as is strictly necessary for the purposes for which it has been provided[17]. In doing so they should also take cognisance of Data Protection Act Principle 4[18]: 'Personal data shall be accurate and, where necessary, kept up to date'.

[13] http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.pdf

[14] In recognition that that publication of a PIA might in certain circumstances compromise the future security of a system, that in such exceptional circumstances certain parts of the PIA might not be published. Seeking a view from the ICO would be sensible and the aim should be to ensure that not publishing the whole PIA will not be at the cost of making its contents anodyne and therefore of limited value to the public.

[15] (ICO, 2009, PIA Handbook Version 2:) "A PIA needs to be distinguished from a privacy or data protection audit. An audit is undertaken on a project that has already been implemented. An audit is valuable in that it either confirms that privacy undertakings and/ or privacy law are being complied with, or highlights problems that need to be addressed. To the extent that it uncovers problems, however, they are likely to be expensive to address and may disturb the conduct of the organisation's business. A PIA aims to prevent problems arising, and hence avoid subsequent expense and disruption."

[16] **Please take note of the *ICO Data sharing code of practice*:** 'The Data Sharing Code of Practice is a statutory code which has been issued after being approved by the Secretary of State and laid before Parliament. The code explains how the Data Protection Act applies to the sharing of personal data. It provides practical advice to all organisations, whether public, private or third sector, that share personal data and covers systematic data sharing arrangements as well as ad hoc or one off requests to share personal data. Adopting the good practice recommendations in the code will help organisations to collect and share personal data in a way that complies with the law, is fair, transparent and in line with the rights and expectations of the people whose data is being shared.' (ICO, 11 May 2011).

[17] Where professional bodies (or equivalent senior management in a sector) have agreed guidance that is compatible with these Principles and they have been embedded, for example the Caldicott Principles within NHS Scotland, then the existing guidance can be followed.

[18] http://ico.org.uk/for_organisations/data_protection/the_guide/information_standards/principle_4

Avoid creating centralised databases of personal information

4.2 Organisations should seek to avoid creating large centralised databases of people's personal information. People's personal data should not be acquired and aggregated in a single place but maintained in separate data stores relevant to their specific business purpose. Organisations or their employees can still draw together personal information held in more than one place, if there is a business need to do so. That is how most public bodies, including the NHS and local government operate at present and it presents a lower risk than aggregating and storing all the personal information in a single place.

Storing personal and transactional data separately

4.3 Public service organisations must as far as possible store information about people's access to services separately from their personal data, to minimise the risk of data loss and to ensure that even if one set of information is accessed improperly, this does not allow access to a wider range of information about individuals. This may be achieved through the avoidance of centralised databases (see 4.2 above).

Controlling access

4.4 Public service organisations should ensure that personal data is held securely (see 2.1c above), that their employees only have access to the minimum personal information they need and that audit records exist of all accesses to, changes to and uses of that data.

Storing identifying information

4.5 Public service organisations must consider whether identifying information needs to be stored in a database at all. In some cases, it might be preferable for people to hold and manage their own identifying information which can be accessed by the public service organisation when it is needed. This could be achieved, for example, by the information being held on a smartcard and accessed when required through a card reader.

Linking information between systems

4.6 Public service organisations should not share personal information unless it is *necessary*. If a public service organisation needs to link personal information from different systems and databases (internally or between organisations), it should avoid *sharing* persistent identifiers; other mechanisms, such as matching, should be considered. If a public service organisation believes that persistent identifiers should be shared, it must publicly explain why. Where identifiers are in common use arrangements should be developed or adhered to, such as those set out in the guidance on the use of the CHI[19]

[19] The use of the CHI (Community Health Index) across the NHS in Scotland http://www.ehealth.scot.nhs.uk/wp-content/documents/Health-and-social-care-CHI-Guidance-version-1-1-Strategy-Board-Approved-June-20131.pdf

5. Data use for Research and Statistics

Recognise that appropriate protection of privacy, efficient use of data, and scientifically sound and ethically robust research and statistics, are all in the public interest.

5.1 Public service organisations should consider the potential benefits of data being used for research and statistics as well as the necessary protections of privacy of individuals to allow this to happen. They should adopt a proportionate approach to decision making whereby actions taken to manage risks to privacy are in proportion to the degree of these risks, and the level of likely benefits. In considering the risks to privacy, both the likelihood of disclosure and the magnitude of harm which would follow should be considered.

5.2 The following options should be considered for striking a balance between the range of public interests at play:

a. Seeking **consent** of data subjects, or, where this is not practicable, approval from an appropriate oversight body.

b. **An appropriate degree of data anonymisation**. Data should be anonymised sufficiently for data controllers to make a reasonable and justifiable risk-based judgement that data can be shared for the production of research or statistics. In making a decision, the data controller should give particular consideration to indirect identifiers (e.g. individual reference numbers), combinations of data (e.g. gender, date of birth and qualifications) and geo-references (e.g. postcode), and seek to strike a balance between the level of risk to privacy and the likely benefits from research or statistics. There are degrees of data anonymisation and reference should be made to the ICO’s Anonymisation Code of Practice for guidance on balancing data utility with privacy protection.

Physical and technical security

5.3 Security of data transfer, storage and use is vital for the protection of privacy, especially where there is any risk of re-identification. Appropriate and proportionate physical and technical security measures should be applied to ensure the confidentiality, integrity and availability of information and should reflect the assessed risk level.

Openness and Accountability

5.4 Information about how and why citizens’ data are being used for statistics and research should be publicly available and, if possible, at the point of collection. If public service organisations are sharing citizens data, the Data Sharing Agreements should be made publically available and citizens should be given adequate opportunity to request further information and raise concerns.

Data Linkage

5.5 Procedures to link data should involve the separation of identifiers (e.g. name, or unique reference number) from the rest of the data, and consideration should be given to separating the indexing, linking and analysis functions and personnel. The linkage method used should be that which requires the minimum necessary identifiable data. The default position should be that data users have access only to data from which names and direct identifiers have been removed, and data users should be subject to an obligation not to attempt to re-identify individual data subjects. Any request for researchers to have access to data containing identifiers should be fully justified and risk assessed. No attempt should be made to re-identify individual data subjects and doing so without the authority of the data controller would be in breach of the Data Protection Act.

6. Education and Engagement

Raise public awareness and understanding

6.1 The Scottish Government should work with public service organisations and others to raise the public's awareness and understanding about the issues covered in these Principles.

Educate people about identity management and privacy issues

6.2 Public service organisations must ensure that staff or contractors who handle personal data on their behalf have and maintain a good working knowledge and understanding of identity management and privacy. This is consistent with Data Controllers remaining responsible for ensuring their processing complies with the Data Protection Act, whether they do it in-house or engage a data processor[20].

6.3 Public service organisations must take steps to ensure that their service users have enough information to make informed decisions about identity management and privacy.[21]

6.4 Public service organisations should remind people (both employees and the public) about the importance of protecting their personal data, including not disclosing their passwords or PINs and not sharing their means of identification with others.

Inform and consult the public

6.5 If a public service organisation is planning or developing a system which involves personal information, it must inform and consult the public and particularly individual users (this is likely to be part of the PIA process). Where children are involved, it will be important to ensure that parents / guardians are also appropriately consulted.[22],[23] Methods of consultation and involvement must match the needs of the audience.[24]

Justify and communicate choices

6.6 Public service organisations must work to build public confidence and trust in their systems and practices. They must explain and communicate why information is

[20] http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

[21] The ICO published a *Code of Practice on Privacy Notices* in June 2009.

[22] Children aged 12 and above are presumed mature enough to exercise their rights under the Data Protection Act 1998.

[23] Biometric identification systems in schools: Guidance for education authorities, learning establishments and schools

[24] Helpful pointers to best practice and innovative methods of public engagement and consultation are available from groups such as Involve (www.involve.org.uk), the International Association for Public Participation (www.iap2.org) and the Consultation Institute (www.consultationinstitute.org).

needed, how it is handled and where and why it is shared[25]. They should also provide a clear explanation of the expected benefits and pitfalls of their authentication mechanisms.

Provide easy access to own data

6.7 Public service organisations should provide simple, quick and effective means for individuals to access information held about them. This might require no more than existing methods used to comply with DPA Subject Access Requests, but could extend to include secure electronic access to check and correct the data that is held on them (any such provision would need to be audited and regulated so that the security and accuracy of data is not compromised).

Duty to repair or redress

6.8 Where an individual demonstrates emotional or material harm arising from incorrect or misused personal information held about them, organisations should assume a duty to repair that information and / or otherwise redress the harm as appropriate.

[25] The ICO published a *Code of Practice on Privacy Notices* in June 2009.

Glossary

Authentication[26]: the process by which the electronic identity of a user is asserted to, and validated by, an information system for a specific occasion using a credential issued following a registration process. It may also involve establishing that the user is the true holder of that credential, by means of a password or biometric. Mechanisms for authentication can include:

- **User name, password and Personal Identification Numbers (PINs)**: These are typically a non-confidential name and a confidential password or number which are shared between a person and a system which may be used alone or together to allow specified access rights to the system.

- **Known Facts**: Information stored by a service provider or organisation to authenticate an individual seeking access to a service, such as current address.

- **Shared Secrets**: A piece of pre-agreed information such as a password or phrase or Questions and Answers, that is only known to the parties involved in a secure communication, such as between an individual and a service provider.

- **Smartcards**: A card containing a microchip which is capable of storing information, such as entitlements to free bus travel.

Encryption: The process of converting information into a code, by using a sequence of instructions (an *algorithm*) to make the information unreadable to anyone except those possessing special knowledge (usually referred to as a *key*).

Identifier: Frequently a sequence of characters and / or numbers that is used and / or assigned by an organisation to a person to identify *uniquely* the person for the purposes of the organisation's systems and operations. A **Persistent Identifier** is an identifier which will remain the same regardless of where the identifier is located, for example, one which is used in several independent databases.

Identity Management: The enrolment and subsequent verification (i.e. the decision made as a result of authentication) that gives individuals trusted means to prove who they are to others and / or are entitled to a service or benefit. An Identity **Management System** is the infrastructure which specifies the ownership, use and storage of information involved in managing identity.

Personal information/data: is as defined in Data Protection Act (and see ICO's guidance[27]).

[26] Adapted from Security - e-Government Strategy Framework Policy and Guidelines Version 4.0 http://webarchive.nationalarchives.gov.uk/20061004085342/http://govtalk.gov.uk/documents/security_v4.pdf

[27] http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

Privacy Impact Assessment (PIA): This is a risk management technique for projects that involve personal information or intrusive technologies, conducted at an early stage of a new project or when a considerable change to a project is planned, to identify and address privacy issues. A PIA helps to explain how an organisation considered privacy in the design and implementation of a system and communicates this to users and people whose information is used. The Information Commissioner's Office (ICO) has published a Code[28] to help organisations decide whether a PIA is appropriate and to help them carry out a PIA.

Public Service Organisations: Is a common term used to describe organisations that use public money to provide public services. This can include organisations from any sector (e.g. public, private or third sector).

Registration[29]: the process by which a user gains a credential such as a username or digital certificate for subsequent authentication. This may require the client to present proof of real-world identity (such as birth certificate, passport) and/or proof of other attributes depending on the intended use of the credential (e.g. proof that an individual works for a particular organisation).

Helpful resources

The ICO's website[30] is the default place to obtain current codes of practice, guidance and useful commentary along with core obligations under the Data Protection Act. This includes the *Data sharing code of practice[31],* the *Subject Access code of practice[32]* and the *Anonymisation: managing data protection risk code of practice[33]*. You may also wish to consider subscribing to the 'ICO e-newsletter'.

[28] http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment

[29] Adapted from Security - e-Government Strategy Framework Policy and Guidelines Version 4.0

[30] www.ico.org.uk

[31] http://www.ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

[32] http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject-access-code-of-practice.PDF

[33] www.ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing