Identity Management and Privacy Principles

Privacy and Public Confidence in Scottish Public Services

The Scottish Government

December 2010

Version 1.0
Contents

Ministerial Foreword ................................................................................................... 3
Information Commissioner’s Statement ................................................................. 4
Introduction................................................................................................................. 5
1. Proving Identity or Entitlement ............................................................................. 6
2. Governance and Accountability ......................................................................... 7
3. Risk Management ............................................................................................... 9
4. Data and Data Sharing ....................................................................................... 9
5. Education and Engagement .............................................................................. 10
Glossary ................................................................................................................... 12
Link to pages to contain examples, case studies and links to helpful resources ...... 13
Ministerial Foreword

The Scottish Government is committed to ensuring that our public services are high quality, continually improving, efficient and responsive to local people’s needs. As we face the most serious budget reductions for at least a generation, we need to respond by reshaping our public services to deliver better outcomes for citizens, but at a reduced overall cost. We need more collaboration, more co-operation, more sharing of resources and services.

However, that does not mean we should ignore people’s rights to have their personal data handled with respect and with due regard to our obligations. Respect for privacy should always be central to the way in which public services manage people’s identity information. I want the public to be able to trust and have confidence in Scottish public services that are not only effective but also secure and privacy-friendly.

Existing data protection and human rights legislation govern personal information management by providing privacy protection. These Identity Management and Privacy Principles have been developed for Scottish Ministers by an expert group1 to help public service organisations comply with such legislation and support good practice. I am particularly grateful for the support of the Information Commissioner’s Office and the time that Ken Macdonald, the Assistant Commissioner for Scotland, has put into their development.

Following a consultation on the draft Principles we published an analysis report on 30 September 2010. The valuable feedback we received both showed that the Principles were broadly welcomed and helped to shape this version of the text.

These Principles form guidance, they are aimed at both public sector policy makers and practitioners concerned with systems for proving identity or entitlement to public services. They neither displace nor create any legal rights or obligations. Along with these high level Principles, policy makers and practitioners should use practical guidance, such as from the Information Commissioner’s Office, in conjunction with technological solutions such as privacy enhancing technologies. These Principles form a ‘living document’ and will be reviewed periodically, for example to ensure compatibility with the UK’s first ever statutory code of practice on data sharing which is currently in draft for consultation2.

I believe these Principles will present a major step forward in helping organisations achieve privacy-friendly Scottish public services, and I expect public sector organisations to embrace them fully.

John Swinney  
Cabinet Secretary for Finance and Sustainable Growth  
December 2010

---

1 The expert group’s members were: Ken Macdonald, Assistant Commissioner for Scotland, Information Commissioner’s Office; Rosemary Jay, Partner at Pinsent Masons LLP; Jerry Fishenden, Lead Technology Advisor, Microsoft UK; Gus Hosein, from Privacy International; Charles Raab, Professor Emeritus and Honorary Fellow at University of Edinburgh; Alan Kirkwood Chair of SocITM Scotland; Duncan Macniven, Registrar General for Scotland; and Kerr Donaldson, Scottish Government.

Information Commissioner’s Statement

As UK Information Commissioner, I have responsibility for ensuring compliance with the Data Protection Act. In that capacity, I welcome the opportunity to contribute a foreword to the Scottish Government’s Identity Management and Privacy Principles.

All organisations handling personal information have a duty under the Data Protection Act to ensure that they handle information appropriately and securely. Unfortunately, as we have seen all too often in the recent past, both public and private sector organisations have frequently failed to meet these obligations. By adhering to these principles, the risk of inappropriate disclosure or loss should be reduced significantly.

The obligations laid on data controllers are not merely bureaucratic or theoretical. Looking after the citizen’s data is part of good administration, efficient service delivery – and respect for clients.

But individuals are not the only losers when the rules are ignored. It would be as well to bear in mind that since April 2010, I have had the power to levy monetary penalties of up to £500k on organisations that breach the Data Protection Act causing substantial harm or distress. In settling on an appropriate penalty, I take into consideration, among other factors, the level of compliance with best practice guidance issued both by my office and by other relevant parties.

I urge that all Scottish public authorities, not just the Scottish Government, adopt these principles as a minimum standard in their handling of personal information and I commend the Scottish Government for taking forward their development.

Christopher Graham
Information Commissioner
December 2010
Introduction

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.

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 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 five sub topics:

1. Proving Identity and Entitlement
2. Governance and Accountability
3. Risk Management
4. Data and Data Sharing
5. 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. The Examples and Good Practice web page will be updated periodically.

---

\(^3\) 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 take into account factors such as legislative requirements and ICO guidance) and that are appropriate to the organisation and function⁴, are used to ensure the security of personal information throughout its lifecycle including while organisations share information right through to archiving it. 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)⁵⁶⁷ 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 necessary⁹ 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 equivalent¹⁰⁸.

---

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.
⁷ ICO’s Data sharing statutory code of practice consultation www.ico.gov.uk/about_us/consultations/our_consultations.aspx
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\(^\text{11}\).

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\(^\text{7}\).

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.\(^\text{12}\) 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 impacts should be submitted for consideration by the lead committee in the Scottish Parliament.


\(^\text{12}\) Data controllers remain responsible for ensuring their processing complies with the Act, whether they do it in-house or engage a data processor.
3. Risk Management

Carrying out Privacy Impact Assessments (PIAs)
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 available13, 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.14

4. Data and Data Sharing

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 provided15. In doing so they should also take cognisance of Data Protection Act Principle 416: ‘Personal data shall be accurate and, where necessary, kept up to date’.

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.

References:
13 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.
14 (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.”
15 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.
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 17.

5. Education and Engagement

Raise public awareness and understanding
5.1 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
5.2 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. 18

18 www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx
5.3 Public service organisations must take steps to ensure that their service users have enough information to make informed decisions about identity management and privacy.19

5.4 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
5.5 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.2021 Methods of consultation and involvement must match the needs of the audience.22

Justify and communicate choices
5.6 Public service organisations must work to build public confidence and trust in their systems and practices. They must explain and communicate why information is needed, how it is handled and where and why it is shared23. They should also provide a clear explanation of the expected benefits and pitfalls of their authentication mechanisms.

Provide easy access to own data
5.7 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
5.8 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.

---

20 Children aged 12 and above are presumed mature enough to exercise their rights under the Data Protection Act 1998.
21 Biometric identification systems in schools: Guidance for education authorities, learning establishments and schools
22 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).
Glossary

Authentication\(^{24}\): 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\(^{25}\)).

---


\(^{25}\) http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx
**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) produced a Handbook 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:** 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).

**Link to pages to contain examples, case studies and links to helpful resources**

We will seek to publish examples and case studies along with providing links to resources you may find useful at www.scotland.gov.uk/privacyprinciples. The ICO's website is the default place to gain current codes of practice and useful commentary along with core obligations under the Data Protection Act.

---
