



Information Governance Policy

Umbrella policy for all
information governance related
policies

V 2.0
October 2015

Governance and Information Service –
Communities and Organisational
Development Directorate

Current Document Status			
Version	2.0	Approving body	Chair of the Information Governance Board
Date	22 March 2016 October 2015	Date of formal approval (if applicable)	21 March 2016
Responsible officer	Sarah White Information Governance Lead	Review date	October 2016
Location			

Version History			
Date	Version	Author/Editor	Comments
12/01/2015	0.1 Draft	Sarah White	First draft for consultation.
30/01/2015	1.0	Gemma Stephenson	Final version
21/10/2015	2.0	Sarah White/Gemma Stephenson	Policy Review

Comprehensive Impact Assessment Record					
Date	Type of assessment conducted	Stage/level completed (where applicable)	Summary of actions taken decisions made	Completed by	Impact Assessment review date
23/01/2014	Initial	Complete	NFA	Sarah White	11/02/2015

Document retention	
Document retention period	Until superseded

Summary

This IG policy provides an overview of the organisation's approach to information governance; a guide to the procedures in use; and details about the IG management structures within the organisation.

This policy covers Information Governance matters in relation to all of the information assets of Cornwall Council.

The Council believes that accurate, timely and relevant information is essential to deliver the highest quality services. As such it is the responsibility of all staff to ensure and promote the quality of information and to actively use information in decision making processes.

There are four linked strands that run through good information governance:

- Openness/transparency
- Legal compliance
- Security
- Quality assurance

Non-confidential information about the Council and its services will be available to the public through a variety of procedures and media.

Service users and others will be given lawful access to information about themselves.

The Council will respect the common law of confidentiality, the right to privacy under the Human Rights Act, the principles and rights set out in the Data Protection Act and the Freedom of Information Act, and will follow as appropriate guidance given by the Information Commissioner and professional and other national bodies.

The Council will establish and maintain policies, procedures, guidance and training to ensure the effective and secure management of its information assets and resources, including information about service-users and others, and about staff.

The Council will establish and maintain policies, procedures, guidance and training for information quality assurance and the effective management of information.

Context

Background

This policy acts as an umbrella policy over other policies relating to elements of Information Governance (IG) that provide more detail about how the different strands are managed within the Council. All of the other policies which fall into the various areas of IG; Confidentiality, Data Protection, Information Security, Freedom of Information, Information Lifecycle, etc, are traceable up to the IG Policy.

Information is a vital asset in terms of both the service the Council provides to customers, and the efficient management of services and resources. It plays a key part in corporate governance, service planning and performance management.

It is of paramount importance that information is effectively managed, and that policies, procedures, structures and accountabilities provide a robust framework for IG.

Objective

This IG policy provides an overview of the Council's approach to information governance; a guide to the procedures in use; and details about the IG management structures.

Scope

This policy covers IG matters in relation to all of the information assets of Cornwall Council. There are many types of information asset the Council is responsible for, including:

- **Information:** customer and service user databases, system documents and procedures, archived information etc.
- **Software:** Applications, system, development tools and utilities.
- **Physical:** Equipment such as PCs, laptops, PDAs, memory sticks, smart phones, information on paper (please see the Information Storage Policy for further details).

Anyone who processes information for the Council or on behalf of the Council must either abide by this policy or prove that they have equivalent policies in place.

Details

Policy Details

Cornwall Council recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Council fully supports the principles of corporate governance and recognises its public accountability, but places equal importance on the confidentiality of, and the security arrangements to safeguard, both personal information about customers, service users and staff and

commercially sensitive information. The Council also recognises the need to share information with outside organisations in a controlled manner consistent with the interests of its customers and service users and, in some circumstances, the public interest.

The Council believes that accurate, timely and relevant information is essential to deliver the highest quality services. As such it is the responsibility of all staff to ensure and promote the quality of information and to actively use information in decision making processes.

The above paragraphs reflect four linked strands that run through good IG:

- Openness/transparency
- Legal compliance
- Security
- Quality assurance

Openness

- Non-confidential information about the Council and its services will be available to the public through a variety of media;
- The Council will establish and maintain policies, procedure, guidance and training to ensure compliance with the Freedom of Information Act;
- Service users and others will be given ready access to information about their rights;
- Service users and others will be given lawful access to information about themselves;
- The Council will have clear procedures and arrangements for handling queries and complaints from service users and others;
- The Council will have clear procedures and arrangements for liaison with the press and other broadcasting media.

Legal Compliance

- The Council will respect the common law of confidentiality, the right to privacy under the Human Rights Act, the principles and rights set out in the Data Protection Act and the Freedom of Information Act, and will follow as appropriate guidance given by the Information Commissioner and professional and other national bodies;
- The Council will establish and maintain policies, procedures, guidance and training to ensure compliance with the above laws, rules and guidance;

- The Council regards all personal information about staff as confidential except where the public interest dictates otherwise.

Information Security

- The Council will establish and maintain policies, procedures, guidance and training to ensure the effective and secure management of its information assets and resources, including information about service users and others, and about staff;
- The Council will promote effective confidentiality and security practice among its staff through policies, procedures, guidance and training;
- The Council will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security;
- The Council will establish and maintain business continuity procedures.

Information Quality Assurance

- The Council will establish and maintain policies, procedures, guidance and training for information quality assurance and the effective management of information;
- All staff have responsibility for the quality of information within their services;
- When possible the quality of information should be confirmed when it is received;
- Where possible common definitions, known as data standards will be set and used to support the sharing, exchange and comparison of information across the public sector.

Management

Policy management

The Governance and Information Service in the Communities and Organisational Development Directorate is the designated Council owner of the IG Policy and is responsible for the maintenance and review of related IG policies such as the Data Protection Policy, the Information Security Policy and the Records Management Policy including associated standards, guidelines and procedures.

It is the role of the Information Governance Board to lead, co-ordinate, monitor, and otherwise ensure the compliance of the Council's social care and public health functions with the NHS IG Toolkit and have regard to the wider implications for IG in the Council, to ensure that information is recorded, used and shared appropriately and securely.

The Directorate IG Groups support each directorate to promote and deliver its commitment to embed IG throughout its services and evidences its direction of travel against relevant IG legislation and compliance standards.

The Corporate Governance and Information Team is responsible for overseeing day to day IG issues; developing and maintaining policies, standards, procedures and guidance, coordinating IG in the Council and raising awareness of IG.

The Freedom of Information Section in the Freedom of Information & Complaints Team based in the Customers and Communities Service is responsible for overseeing day to day issues relating to the Council's compliance with the Freedom of Information Act 2000.

The Council's Senior Information Risk Owner (SIRO) is responsible for managing corporate information risks, including maintaining and reviewing an information risk register.

The Caldicott Guardian plays a key role in ensuring that the Council's social care and public health functions apply the highest standards when handling personal information. The Guardian supports good information sharing, advises on the lawful and ethical use of information, and acts as the conscience of the Council.

The Council's Internal Audit Service will review the adequacy of the controls that are implemented to protect the Council's information and recommend improvements where deficiencies are identified.

Heads of Service and departmental managers are responsible for ensuring that staff are made aware of and comply with the Information Governance Policy, Standards, Guidelines and Procedures.

Users accessing Council information are required to adhere to the Information Governance Policy, Standards, Guidelines and Procedures.

Breaches and non-compliance

Any breaches of this policy may lead to disciplinary action being taken. Serious breaches of this policy by Council employees will amount to gross misconduct and may result in dismissal.

Where external service providers, agents or contractors breach the policy, this should be addressed through contract arrangements.

If you see a breach of this policy, you must report it using the [security incident reporting form](#).

How the impact of the policy will be measured

The Corporate Governance and Information Team will monitor compliance with the policy and performance with regard to information governance. Indicators to monitor the performance on IG are:

- Annual Internal Audit of the NHS Information Governance Toolkit to ensure effectiveness of procedures that provide a moderate level of assurance;
- Number of adverse judgements from the ICO linked to information governance issues.

Potential risks will be regularly monitored and evaluated to ensure this policy is kept up to date.

The policy must be reviewed 3 months prior to new legislation taking effect.

Evaluation and review

This policy will be reviewed every three years or as demanded by business need by the management team of Governance and Information and the Information Governance Board.

This policy will be signed off by the Chair of the Information Governance Board.

Authority is delegated to the Head of the Governance and Information Service to undertake amendments of an administrative nature as are necessary, or to secure continuing compliance with the law.

Document information

Contacts

Policy prepared by Sarah White, Information Governance Lead

Further information

Users should read this policy in conjunction with the following Council policies, procedures and guidance:

- [Data Quality Guidelines](#)
- [Data Protection Policy](#)
- [Confidentiality Policy](#)
- [Information Security Policy](#)
- [Information Security breach reporting procedure](#)
- [Information Storage Policy](#)
- [Freedom of Information Policy](#)
- [Information Access Request Procedure](#)
- [Subject Access Procedure including Section 29 procedure](#)

Alternative formats

If you would like this information in another format please contact:
Cornwall Council, County Hall, Treyew Road, Truro TR1 3AY

Telephone: **0300 1234 100** email: enquiries@cornwall.gov.uk

www.cornwall.gov.uk

Please consider the environment. Only print this document if it cannot be sent electronically.