

# Information Compliance Policy

**Version:** 2.0

**Date Issue:** January 2015

**Review date:** January 2016

**Reference:** WCCC-1073-234

**Team:** Information Management

**Protective Marking:** Public

© Warwickshire County Council 2015

# Contents

**Introduction..... 3**

**The policy..... 4**

    Protecting personal and confidential information..... 4

    Creating, storing and managing information..... 4

    Giving access to information ..... 4

    Sending and sharing information..... 4

    Preserving and disposing of information ..... 5

    Accessing information using IT equipment, systems and applications..... 5

    If things go wrong..... 6

    Training ..... 6

**Responsibilities ..... 6**

**Monitoring and review ..... 7**

**Further Information ..... 7**

**Appendices ..... 8**

    WCC information standards and procedures ..... 8

    WCC related policies..... 8

    External legislation ..... 8

## Approvals

v1	Corporate Board	26 November 2014
v2	Information Governance Steering Group	9 December 2014
v2	Strategic Director for Resources / Monitoring Officer	January 2015

## Introduction

This policy sets out the statement of intent that Warwickshire County Council (WCC) and its staff will follow with regard to information compliance. The policy and associated standards and procedures are **mandatory** and must be followed by all staff as part of the council's [Information Governance Framework](#).

Our [Information Rights policy](#) sets out the rights the public and employees have to access personal and public information. *“We hold personal information to provide services to individuals and an individual has a right to request access to their records and information held about them. An individual should be confident that we handle your personal information responsibly and in line with good practice. Where possible we make available public information through our website, in leaflets and on demand.”*

Staff must ensure they apply this policy and good information governance to all their work and information they handle, as we have a duty to the public as well as complying with legislation.

“Staff” includes all employees, Councillors, secondees, volunteers, work experience and any other individuals working for the Council on a contractual basis.

Information is used here as a collective term to cover terms such as data, documents, records and content.

Personal information means any identifiable data or information in paper or digital format, relating to a living or deceased individual.

Council information includes any data or information that is held by us on behalf of individuals, business, partners or we create in order to carry out our services.

Confidential information includes personal information and any other council information that is deemed to be restricted and not released or shared without safeguards in place.

## **The policy**

### **Protecting personal and confidential information**

We will meet our obligations in line with the principles of the Data Protection and Human Rights Acts and other relevant legislation, recognising the rights to privacy of living and deceased individuals.

We will need to share some personal data in order to deliver services, perform our duties and legal obligations but will only do so where we have permission or a legal power to do so.

We will provide notices which explain why we collect personal information and how we use and share information.

Staff will process and keep personal and confidential information safe and secure at all times, including at the office, public areas, home or in transit. Such information will not be divulged or discussed except in the performance of normal work duties.

Staff will consider and address the risks to personal information when we are planning to use or hold personal information in new ways, introducing new systems or collecting more personal information.

### **Creating, storing and managing information**

Staff will classify and use information according to its risk, sensitivity, value, and importance while considering who should receive or have access to it. Staff will use WCC and service standards and procedures for assessing information risk, applying protective markings and handling.

Staff will only store personal and council information in approved locations (e.g. paper archives, office cabinets, devices, networks, systems). Staff will not store council information permanently at home if paper or on their own unencrypted devices if electronic.

Staff will consider the audience and presentation format to make information accessible.

### **Giving access to information**

Staff will respect people's right to access personal and public information that the council creates, owns or holds and assist them in accessing it.

Staff will provide access to personal information where the law allows or requires us to do so, or with consent.

### **Sending and sharing information**

Staff will follow WCC and service standards and procedures for sending or sharing personal and confidential information outside the council including use of secure email and encryption for sending electronic information and tracking for paper documents.

Staff will follow sharing procedures where a sharing agreement is in place.

## **Preserving and disposing of information**

We will only retain information for the time period applicable to the type of information using WCC and service standards for retention/disposal. This applies to both paper and electronic information.

For information deemed worthy of preservation for historical/research purposes, we will retain permanently in council archives.

Staff will use the Records Management archive service for paper files that are no longer in active use but need to be retained.

Staff will dispose of paper and electronic information classified as personal or confidential using confidential waste procedures.

## **Accessing information using IT equipment, systems and applications**

Staff will only access personal information that is necessary for their role and business need.

Staff will keep their individual WCC accounts and their id/passwords for their own use - and not share with others.

Staff will make use of strong passwords that conform to the minimum standard, when accessing system accounts, applications and encrypted devices. Staff must not disable password protection standards.

Staff will 'lock' computer screens on any device or log-out/shutdown before leaving any workstation or device unattended.

Staff will keep all WCC supplied mobile/portable computing equipment locked away when left on WCC premises overnight and take all reasonable measures to keep equipment locked away, secure and out of sight when taken out of WCC premises.

Staff will only purchase and use assets (hardware, software, applications and services) that are approved by Information Assets for WCC business, to ensure information risks are assessed, confidential information is secure and the assets are all registered.

Staff will only use authorised software and applications approved by Information Assets.

Staff will not allow unauthorised access to WCC equipment and information, or knowingly introduce any security threat.

Staff and their managers will ensure that all council information and equipment they own or hold is transferred or returned before leaving the council.

## **If things go wrong**

Staff will report any potential or actual losses of information or equipment holding information, potential or actual security incidents (e.g. inappropriate access, hacking, misuse of password, viruses), using the council incident reporting procedure.

We will investigate reported incidents and information breaches and assist those conducting investigations and take appropriate action.

## **Training**

We will provide training for all Staff on information rights and compliance, appropriate to the role and use of information, at induction and at least every two years.

Staff will consult and seek advice from their line manager if further training or guidance is required, who will arrange further training or support.

## **Responsibilities**

Warwickshire County Council is the overall body responsible for providing information, with the legal obligations being enforced by the Information Commissioner and the courts.

Specific responsibilities for all staff within the council are as follows:

- Awareness of the relevant legislation relating to requests for information.
- All staff are responsible for adhering to this policy and any associated standards and procedures.
- All managers are responsible for the implementation and adherence of this policy and any associated standards and procedures within their service and teams.
- Disregard for this policy by employees may be regarded as misconduct to which the council's Dismissal and Disciplinary Procedure applies and a serious breach of any policy may be treated as gross misconduct and may lead to dismissal. Disregard by contractors and agents working for the council will be regarded as a contractual breach. Disregard by volunteers and work experience students working for the council may lead to terminating their work agreement.

All Information in the possession of, or under the control of WCC, will have a designated Information Asset Owner who is ultimately responsible for the protection of their respective information. Heads of Service as Information Asset Owners are accountable for knowing what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information.

Group Leadership Teams are accountable for the effective management of

information risk and information governance compliance, as well as supporting and promoting the policies, standards and procedures.

## Monitoring and review

This policy and the supporting standards will be monitored and reviewed annually in line with legislation and codes of best practice.

An Equality Impact Assessment on this policy was undertaken on 19 August 2014 and will be reviewed in August 2017, or before if required.

## Further Information

Standards and procedures, training and guidance for staff:

[www.warwickshire.gov.uk/im](http://www.warwickshire.gov.uk/im)

Information rights and public access to information:

[www.warwickshire.gov.uk/accesstoinformation](http://www.warwickshire.gov.uk/accesstoinformation)

Information Management, Information Assets, Resources Group,

Shire Hall, Warwick, CV34 4RL

Telephone: 01926 418633

## Appendices

### **WCC information standards and procedures**

*These include but may be added to or replaced and subject to regular updates – refer to [www.warwickshire.gov.uk/im](http://www.warwickshire.gov.uk/im) for the latest version.*

Safe haven / handling procedures  
Information risk and protective marking standard  
Security incident reporting procedure  
Access requests procedure  
Confidentiality and disclosure code  
Information sharing procedure  
Paper archive procedure  
Privacy notices standard and procedure  
Privacy impact standard and procedure  
Encryption/password standards

### **WCC related policies**

WCC information governance framework  
WCC information rights policy  
WCC employee and employer responsibilities code  
WCC terms and conditions of employment  
WCC accommodation standards - section 4, clear desk policy

### **External legislation**

Including:

[Data Protection Act 1998](#)

[Human Rights Act 1998](#)

[Freedom of Information Act 2000](#)

[Environmental Information Regulations 2004](#)

[Local Government Acts](#)

[Copyright, Design and Patents Act 1998](#)

[Computer Misuse Act 1990](#)

**Common Law - Duty of Confidentiality**

This is not a written Act of Parliament. It is “common” law. This means that it has been established over a period of time through the Courts.

It recognises that some information has a quality of confidence, which means that the individual or organisation that provided the information has an expectation that it will not be shared with or disclosed to others.

For information to have a quality of confidence it is generally accepted that:

- it is not “trivial” in its nature
- it is not in the public domain or easily available from another source
- it has a degree of sensitivity
- it has been communicated for a limited purpose and in circumstances where the individual or organisation is likely to assume an obligation of confidence. For example information shared between a social worker/client, health practitioner/patient, etc.

However, as with the Human Rights Act, confidentiality is a qualified right. The Council is able to override a duty of confidence when it is required by law, or if it is in the public interest to do so.