Information Asset Change Policy and Procedure

Document Control

Reference Number	**Version** 2.1	**Status** Published	**Sponsor(s)/Author(s)** Tim Way
Amendments	Removal of word document version of the change request form, introduction of the online version. Removal of out of date protective marking.		
Document objectives: The purpose of this policy is to establish management direction and high-level objectives for change management and control			
Intended Recipients: None			
Group/Persons Consulted: None			
Monitoring Arrangements and Indicators: None			
Training/Resource Implications:			
Ratifying Body and Date Ratified	Information Governance Programme Board		
Date of Issue	Feb 2017		
Review Date	Feb 2018		
Contact for Review	Information Governance		
SIRO signature			

Associated Documentation

Policies - Wiltshire Council controlled documents

- Information Governance Policy
- Information Governance Management Framework
- Network Security Policy
- Mobile Working Policy
- System Level Security Policy
- Incident Management Policy
- Records Management Policy
- Information Asset Policy
- Data Protection and Subject Access Policy
- Privacy Impact Assessment Policy

Legal framework

- Data Protection Act 1998 (and subsequent Special Information Notices)
- Human Rights Act 1998
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988 (as amended) by the Copyright (Computer Programmes) Regulations 1992
- Crime & Disorder Act 1998
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- Health and Social Care Act 2012
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations 2000)
- Public Interest Disclosure Act 1998
- Prevention of Terrorism (Temporary Provisions) Act 1989 & Terrorism Act 2000
- Regulations under Health & Safety at Work Act 1974
- Transparency Code 2015

Contents

1. Introduction

Wiltshire Council manages a variety of information assets which are essential for service delivery. These include key information processing systems (including paper) e.g. operating systems, application systems, hardware and data collection systems.

The council has statutory and regulatory requirements to ensure its information systems and supporting processes meet security, confidentiality, data protection and data quality needs.

An essential requirement for any change management system is the establishment of an accurate and up to date Information Asset Register which lists all of the information, information systems, current data stores and databases used in the delivery of services. Heads of Service as Information Asset Owners(IAOs) are responsible for maintaining this Information Asset Register. IAOs are also responsible for:

- identifying any inward and outward flows of information in their service;
- managing information risks in their service area;
- ensuring any new systems or changes to systems are assessed for privacy compliance prior to implementation.

This policy establishes a formal mechanism for the approval of new information assets and potential changes to existing assets and processes. This will provide assurance to the SIRO that security, confidentiality, data protection and data quality issues have been considered for any new or re-configured asset, system or business process.

2. Scope of the Procedure

The document covers procedures to be adopted when any significant change or addition is made to the council’s information assets.

The policy applies to all members of staff engaged by the council.

The policy covers changes which will have an effect on information systems (paper and electronic) or a significant change to information collection processes. Examples of a major change would be the introduction of a new data warehouse or commissioning an external company to provide a service or process data on behalf of the council.

The development of new information systems or the creation of any new data stores will need to be reflected in the Information Asset Register.

3. Purpose of the Procedure

The purpose of the procedure is to ensure any changes to services are communicated and managed with due consideration given to compliance with confidentiality, data protection and data quality requirements.

This document sets out a formal, process which requires Information Asset Owners to notify intended significant changes to the Information Governance Assurance Group (IGASG), through the completion of the Change Notification Form and the IG Checklist (See Appendix A.) This will reveal areas which need further work or development.

The initial assessment of privacy risks will indicate whether a Privacy Impact Assesment(PIA) is required. A PIA is a process which helps assess privacy risks in the collection, use and disclosure of information. Guidance is provided in the PIA Code of Practice produced by the Information Commissioner's Office (ICO). See also the council PIA policy and PIA Template.

4. Process to be followed

- The Information Asset Owner is responsible for deciding if a proposed change is significant using the criteria given in Section 5.
- For all significant information asset changes the Change Notification Form should be completed. Notification should occur as early as possible so information governance requirements and any potential costs can be included into business cases.
- For all significant information asset changes, the manager responsible for implementing the project will complete the IG Checklist (Appendix B) and send it to the Information Governance Team using the email address information.assurance@wiltshire.gov.uk. The IG Checklist must be completed during the project design phase before any procurement or project implementation activities take place.
- The Information Governance Manager will decide if a Privacy Impact Assesment is necessary after submission of the Change Notification Form or the IG Checklist.
- All signifcant changes will be reported to the Information Governance Assurance Group. When a PIA is required, the IGASG will review and formally approve measures developed to reduce any privacy risks identified by the PIA process.
- At any stage of a business change or project, the Information Governance Manager may refer a serious information governance risk to the IGASG for review.

5. Significant changes to information assets

A change to an information asset is significant when:

- It involves Personal-Sensitive information from the table below, or
- It involves Personal information from the table below and one more of the statements in the following list also applies.

Personal	Personal-Sensitive
Name	Racial / ethnic origin
Address (home or business)	Political opinions
Postcode	Religious beliefs
NHS No	Trade union membership
Email address	Physical or mental health
Date of birth	Sexual life
Payroll number	Criminal offences
Driving Licence [shows date of birth and first part of surname]	Biometrics; DNA profile, fingerprints
	Bank, financial or credit card details
	Mother’s maiden name
	National Insurance number
	Tax, benefit or pension Records
	Health, adoption, employment, school, Social Services, housing records
	Child Protection
	Safeguarding Adults

- A new category of information is being collected or a larger quantity of information is being collected than previously.
- Information is being shared with an organisation which previously has not had routine access to the information. This includes any means of sharing such as paper, removable media, email, SharePoint or direct system to system connection.
- The information will be stored or processed by a new organisation (e.g. cloud hosting)
- Existing information is being used for a purpose that it has not previously been used for.
- New technology is being used which may be perceived as privacy invasive e.g. biometrics,automatic facial recognition
- The justification for any new data handling is not clear or not well understood by the data subjects involved or the justification has not been published.
- The project is partnership based and involves multiple organisations controlling the information.
- There are new or changed requirements for the retention of information.

- The project involves technology changes which may impact on the security of the council's network and IT infrastructure.
- The change will have an adverse effect on the timeliness, completeness or accuracy of information being collected.
- The change will have an adverse impact on the timely access to information for Subject Access Requests

Routine software updates to systems which do not meet any of the criteria given above are not a significant information asset change.

Information Asset Owners should consult the Information Goverance Team for advice if they are uncertain if a proposed change is significant or not.

6. Responsibilities

All staff need to work together to help identify and mitigate information risk. Managing information risk effectively requires a structured approach where accountability sits with business managers, rather than specialist staff. The Information Governance Management framework and Information Asset Policy set out the council's framework of accoutability.

Development of information goverance measures should be carried out by those staff with the best knowledge of a planned or existing information asset with advice from information Governance specialists where necessary. Therefore it is important :

- The Information Governance Team are involved to ensure compliance with security, confidentiality and data protection issues.
- Caldicott Guardians are consulted regarding the exchange and use of social care personally identifiable data and the need for Information Sharing Agreements
- The Information Asset Owner is involved at an early stage in the development of new or re-configured systems to ensure effective security controls are identified, implemented properly and tested.

7. Procedure Awareness

It is the responsibility of the Information Goverance Manager to make all relevant managers aware of the procedure, explain its implications and ensure that it is made available on the intranet.

8. Monitoring and Control

The Information Governance Manager will monitor the introduction of new services and the compliance with the procedure. Failure to use the procedure will be recorded and appropriate follow-up action taken.

Appendix A - IG Checklist: Areas to be considered when introducing new, or changing existing systems

No	Applicable to	Area for consideration	Yes/No	Further work needed	Reference document
A	**General**				
A1	New or Change	Have the Information Governance Team been informed of the planned new/changed system or process?			Terms of Reference of Information Governance Group:- Contact IG lead
A2	New	Have staff accessing the information undertaken appropriate information governance training?			Information Governance Policy
B	**Confidentiality/Data Protection**				
B1	New or Change	Has the 'data controller' been clearly identified?			Data Protection Policy
B2	New or Change	Does the system contain data that would be subject to Subject Access/Access to other Personal Records requests?			Data Protection policy Freedom of Information Policy
B3	New or Change	Will protocols be required to govern the sharing of information with other parties? Are appropriate contractual clauses in place (where applicable)?			Information Governance Toolkit Requirement Information Sharing Protocol.
B4	New or Change	If required are there processes in place to obtain data subject consent for holding/sharing their information?			Data Protection Policy

No	Applicable to	Area for consideration	Yes/No	Further work needed	Reference document
B5	New or change	Are processes in place to inform data subjects how their information will be used at the time they are asked to provide it (Privacy Notice)?			Data Protection Policy
C	**Data Quality**				
C1	New or Change	Will change impact on the quality of the data e.g. its completeness, accuracy, relevance, accessibility, timeliness and validity?			Data Quality Policy
C2	New	Does the system have the ability to record and verify any reference number?			
C3	New	Has consideration been given to methods of data reconciliation and validation?			Data Quality Policy
C4	New	Are national or locally defined data standards being used wherever possible?			Data Quality Policy
C5	New	Where different systems are recording the same data, are processes in place to ensure there are no inconsistencies between them?			Data Quality Policy
C6	New	Can changes to records be tracked to identify who has made the change i.e. audit trail in electronic			Data Quality Policy/ Information Security Policy

No	Applicable to	Area for consideration	Yes/No	Further work needed	Reference document
		system, signed changes in paper records?			
D	**Information Security**				
D1	New	For procurements, has the relevant security evaluation questionaire been included in the requirements?			Information Security Policy
D2	New	Are relevant security systems in place to ensure that identifiable information is protected from unlawful or unauthorised access e.g. appropriate access controls,system monitoring and alerting, security patching, restrictions on bulk data export, encryption of data at rest?			Information Security Policy
D3	New	Have processes been considered to protect information from accidental loss, destruction or damage?			Information Security Policy
D4	New	Are controls in place to physically protect assets and ensure availability of utilities and services?			Information Security Policy
D5	New	Are controls in place to protect the system/network from malicious software?			Information Security Policy
D6	New or change	Are backup processes in place, or will they be developed? Do these			Information Security Policy

No	Applicable to	Area for consideration	Yes/No	Further work needed	Reference document
		align with information availability requirements?			
D7	New or change	If data is transferred, is appropriate encryption in place to ensure the secure transfer of routine information flows?			Information Security Policy / Protective Marking Policy
D8	New	Are access controls in place?			Information Security Policy
E	**Records Management**				
E1	New or /Change	Will changes/introduction of new system impact on the ability to dispose, retain or archive information?			Records Management Policy Retention & Disposal Schedules
E2	New	Is there an agreed retention/destruction period (based on local agreement or legal minimum retention periods)?			Records Management Policy and associated procedures
F	**Freedom of Information**				
F1	New/Change	Does the system contain information which may be subject to Freedom of Information requests?			Freedom of Information Policy and Procedure