Corporate Policy and Resources Committee
9 February 2017

Subject: Information Governance Policy Review

Report by:	Director of Resources
Contact Officer:	Steve Anderson Information Governance 01427 676652 Steve.anderson@west-lindsey.gov.uk
Purpose / Summary:	To report on progress of the review of information governance policy documents being carried out by the Corporate Information Governance Group and to request approval from the CP&R Committee for reviewed policies to be implemented for all staff, elected members, and partners where appropriate.

RECOMMENDATION(S):

1. That Members approve the attached information policies for implementation to all staff, elected members, and partners where appropriate.

2. That delegated authority be granted to the Director of Resources to make minor housekeeping amendments to the policy in future, in consultation with the chairs of the Corporate Policy & Resources Committee and Joint Staff Consultative Committee.

IMPLICATIONS

Legal: We are required by legislation such as the Data Protection Act 1998 to implement and maintain policies on the management and protection of information.

Financial : None – Fin/129/17

Staffing : None

Equality and Diversity including Human Rights :

These new policies have no impact, adverse or otherwise, on any particular group.

Risk Assessment : None

Climate Related Risks and Opportunities : None

Title and Location of any Background Papers used in the preparation of this report:
N/A

Call in and Urgency:

Is the decision one which Rule 14.7 of the Scrutiny Procedure Rules apply?

i.e. is the report exempt from being called in due to urgency (in consultation with C&I chairman)	**Yes**		**No**	**X**

Key Decision:

A matter which affects two or more wards, or has significant financial implications	**Yes**		**No**	**X**

1. **Background**

In order to safeguard the Council's vital information assets and comply with the extensive legal framework around information and privacy, the Council is required to put in place an Information Security Management System (ISMS) based on recognised industry standards such as ISO/IEC 27001 (Information Security Management Systems) at the heart of its information governance activities. The Local Public Services – Data Handling Guidelines (4th Edition (November 2016)) recommends that local authorities structure these activities around 5 headings:

- Policy
- People
- Places
- Partnerships
- Processes/Procedures

Accountability for the Council's Information Assurance and ISMS rests with the Director of Resources through his role as the Senior Information Risk Owner (SIRO). He delegates responsibility for information governance to the Corporate Information Governance Group (CIGG) which he chairs. The CIGG is comprised of the information specialists from across the Council who meet approximately 6-weekly to share good practice, monitor compliance, and maintain elements of the Council's ISMS.

Comprehensive and up-to-date policies are essential to influence decisions on which security controls we need, inform the development our processes and procedures, and define training and awareness objectives for our staff, councillors and partners. Policies are usually the first thing asked by auditors when they are assessing particular aspects of our information governance arrangements.

This is the first in a series of reports covering a complete review of the Council's information policies currently being undertaken by the CIGG and scheduled for completion by end May 2017.

The attached Policies have been reviewed and agreed by the Governance Corporate Leadership Team (GCLT) and were supported by members, unions and staff representatives at the Joint Staff Consultative Committee (JSCC) on 30 Jan 2017.

2. **The Policy Review**

The Council's information policy set is broken down as follows:

Information Management Policies

Title	Document Owner	Review Date
Data Protection Breach Policy	Emma Redwood	16/01/2015
Data Protection Policy	Emma Redwood	27/08/2015
Data Quality Policy	James O'Shaughnessy	19/02/2016
Freedom of Information and Environmental Information Policy	Emma Redwood	27/08/2015
Information Governance Policy	Steve Anderson	27/10/2018
Information Management and Protection Policy	Steve Anderson	23/06/2015
Information Sharing Policy	Steve Anderson	27/10/2018
Legal Responsibilities Policy	Steve Anderson	27/10/2018
Privacy Notice	Steve Anderson	05/01/2016
Records Management Policy	Steve Anderson	16/01/2015

Note: Shaded policies are not due to be reviewed.

Information Security Policies

Title	Document Owner	Review Date
Information Security Policy	Cliff Dean	23/06/2015
IT Access Policy	Cliff Dean	15/08/2014
IT Infrastructure Security Policy	Cliff Dean	15/08/2014
Remote Working Policy	Cliff Dean	23/06/2015
Removable Media Policy	Cliff Dean	16/01/2015
Internet Acceptable Usage Policy	Cliff Dean	23/06/2015
Bring Your Own Device Policy	Cliff Dean	30/11/2016
Computer Telephone and Desk Use Policy	Cliff Dean	15/08/2014
Email Policy	Cliff Dean	30/11/2016
Email Policy for ActiveSync Users	Cliff Dean	30/11/2016
Information Security Incident Management Policy	Steve Anderson	01/12/2016
Mobile Device Policy	Cliff Dean	16/04/2016
PSN AUP and Personal Commitment Statement	Cliff Dean	29/08/2014

This report covers the 5 documents completed so far as detailed below:

a. Data Protection Policy

The Data Protection Policy is part of the Council's Information Management Policy Framework and sets out the principles of data protection; our responsibilities; the access rights of individuals; information sharing; and how we shall deal with complaints. It is a mandatory requirement to comply with the Data Protection Act 1998.

It applies to all full time and part time employees of West Lindsey District Council, elected members, partner agencies, contracted employees, third party contracts (including agency employees), volunteers, and students or trainees on placement with the Council.

The primary changes introduced as a result of the review are:

1. To recognise the appointment of the Monitoring Officer to the role of Data Protection Officer for WLDC.
2. Responsibility for data protection administration activities assigned to Team Manager, Customer Strategy and Support.

Full details of changes made in this new version are at Appendix 1.

b. Information Management and Protection Policy

Information is a principal asset of the Council. The Information Management and Protection Policy is part of the Council's Information Management Policy Framework and is an over-arching policy on which all information-related activity is built. It aims to allow information to be managed and protected from creation or acquisition to destruction or permanent archive, taking into account its security, storage, access, distribution, use, presentation and retention.

It applies to all full time and part time employees of West Lindsey District Council, elected members, partners, contracted employees, third party contracts (including agency employees), volunteers, and students or trainees on placement with the Council.

The primary changes introduced as a result of the review are:

1. Updates to reflect new Government security classifications
2. Changes to the Council's governance structure reflected in the Policy.

Full details of changes made in this new version are at Appendix 2.

c. Data Quality Policy

The Data Quality Policy is part of the Council's Information Management Policy Framework. We are committed to high standards of data quality. We take every care to ensure that the data and information used throughout the organisation and in particular in performance management

is **accurate, valid, reliable, timely, relevant, secure, accessible,** and **complete**.

The Policy provides an overarching, corporate approach to the management of data quality. Service specific procedures will flow from this corporate policy, where relevant and necessary, ensuring that standards outlined in it are maintained throughout the Council.

The Policy is mainly aimed at officers and members of the Council but it applies equally to data used by the Council's strategic partnerships.

The primary changes introduced as a result of the review are:

1. Policy revised to include new Corporate Plan themes and to remove old priorities.
2. Changes to the Council's governance structure reflected in the Policy.

Full details of changes made in this new version are at Appendix 3.

d. Remote Working Policy

The Remote Working Policy is part of the Information Security Policy Framework and it states the Council's policy when accessing ICT resources from outside the security of the Council's offices. It should be read and applied with the Council's Flexible Working Policy and/or Homeworking Policy. Personal Electronic Devices (PED) are provided to assist users to conduct official Council business efficiently and effectively. This equipment, and any information stored on PEDs, should be recognised as valuable organisational information assets and properly safeguarded.

The Policy applies to all councillors, committees, departments, partners, employees of the Council, contractual third parties and agents of the Council who use the Council Information and Communication Technology (ICT) facilities and equipment remotely. The document also applies to anyone who needs remote access to Council information systems or information.

The primary changes introduced as a result of the review are:

1. Changes to the Council's governance structure reflected in the Policy.

Full details of changes made in this new version are at Appendix 4.

e. IT Access Policy

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding

against unauthorised use. Formal procedures must control how access to information is given and how that access is changed. This document sets out the Council's policy with regard to access control and also mandates a standard for the creation of strong passwords, their protection and frequency of change.

The Policy applies to all councillors, committees, departments, partners, employees of the Council (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the Council with any form of access to the Council's information and information systems.

The primary changes introduced as a result of the review are:

1. Password policy completely revised to adopt new Government guidance designed to help users cope with "password overload". Policy now mandates longer, more secure passwords which have to be changed less frequently.
2. References to "Systems Access Forms" removed and replaced with a more generic title, "Requests for Access".
3. Policy now reflects that request for access to ICT systems are now initiated by People and Organisational Development.

Full details of changes made in this new version are at Appendix 5.

3. **Decisions Required**

That Members approve the attached information policies for implementation to all staff, elected members, and partners where appropriate.

Delegated authority be granted to the Director of Resources to make minor housekeeping amendments to the policy in future, in consultation with the chairs of the Corporate Policy & Resources Committee and JSCC.

Appendix 1 - Data Protection Policy Revisions

Policy Title: **Data Protection Policy** New Version: 3.0

Applicable to: Members: Y

Staff (permanent, temporary, placements): Y

Partners: Y

Revisions:

a.	**ADDITION**	Para 1.2	Elected Members.
b.	**ADDITION**	Para 2.1	"Volunteers" to list of people policy applies to.
c.	**AMENDMENT**	Para 2.3	"S: P: drive filing structure" replaced with "shared and personal network drives".
d.	**ADDITION**	Para 2.5	"Elected Members" to list of people we collect data from
e.	**ADDITION**	New Para 4.2	"The role of Data Protection Officer is held by the Council's Monitoring Officer. "
f.	**ADDITION**	Para 4.4	"Strategic Leads" added to list of people responsible for business areas (2 x additions)
g.	**ADDITION**	Para 4.5	New sentence "The responsibility for providing day-to-day advice and guidance to support the Council in complying with the DPA and this Policy rests with the Data Protection Officer."
h.	**AMENDMENT**	Para 4.5	Job title "Member and Support Services Team Manager" replaced with "Team Manager, Customer Strategy and Services".
i.	**AMENDMENT**	Para 5	List of related policies completely revised.
j.	**AMENDMENT**	Para 8.1	Job title "Member and Support Services Team Manager" replaced with "Data Protection Officer".
k.	**AMENDMENT**	Para 12.1	Job title "Member and Support Services Team Manager" replaced with "Data Protection Officer".
l.	**AMENDMENT**	Para 13.2	Job title "Member and Support Services Team Manager" replaced with "Data Protection Officer". (2 x amendments)
m.	**AMENDMENT**	Para 15.1	Policy Review period increased from "1 year" to "2 years".

Appendix 2 - Information Management and Protection Policy Revisions

Policy Title: **Information Management and Protection Policy**

New Version: 5.0

Applicable to:

Members:	Y
Staff (permanent, temporary, placements):	Y
Partners:	Y

Revisions:

a.	**ADDITION**	Para 1	Elected Members.
b.	**DELETION**	Para 3 bullet 4	Deleted in Toto. (Referred to old Government Classification Scheme)
c.	**ADDITION**	Para 3 bullet 5	Added "they have read all relevant Information Governance Policy documents, have completed relevant awareness training," to key message.
d.	**AMENDMENT**	Para 3 bullets 6 and 7	Amended to reflect new Government Classifications.
e.	**ADDITION**	Para 3 bullet 9	Added reference to Information Security Incident Management Policy
f.	**ADDITION**	Para 6.2	5 new risks included and added to the Corporate Risk Register
g.	**AMENDMENT**	Para 8.1	List of related policies completely revised.
h.	**AMENDMENT**	Para 11	Completely revised to reflect new governance structure.
i.	**AMENDMENT**	Para 12.2	"HR Department" amended to "People and Organisational Development Department"
j.	**AMENDMENT**	Para 14.1	Policy Review period increased from "1 year" to "2 years".
k.	**AMENDMENT**	Appendix 1	Diagram updated to reflect current framework.
l.	**AMENDMENT**	Appendix 2 Para 2.1.2	Completely revised to reflect new Government Classifications.
m.	**ADDITION**	Appendix 2 Para 2.1.3	New para added: "Key Classification Principles".
n.	**AMENDMENT**	Appendix 2 Para 2.1.6	Title amended from "Unclassified Information Assets" to "Information of Limited or No Practical Value".
o.	**DELETION**	Appendix 2 Para 2.1.9	Deleted "Software Policy" from list of policies.
p.	**AMENDMENT**	Appendix 2 Para 2.3.2	Amended to reflect new Government Classifications.

Appendix 3 - Data Quality Policy Revisions

Policy Title: **Data Quality Policy** New Version: 2.0

Applicable to: Members: Y

Staff (permanent, temporary, placements): Y

Partners: Y

Revisions:

a.	**AMENDMENT**	Para 1	Para completely revised to include new Corporate Plan themes and to remove old priorities.
b.	**DELETION**	Para 4	Appendix 1 (list of Council key business systems) deleted in Toto.
c.	**ADDITION**	Para 6	Reference to the Council's Legal Responsibilities Policy added and relevant legislation added to list.
d.	**AMENDMENT**	Para 7.1 (Table of roles and responsibilities)	Directors – "responsibility" replaced with "accountability".
e.	**AMENDMENT**	Para 7.1 (Table of roles and responsibilities)	Corporate Governance Team – "CLT" amended to "GCLT".
f.	**AMENDMENT**	Para 7.1 (Table of roles and responsibilities)	Team Managers – reference to "Head of Service" replaced with "Strategic Leads".
g.	**AMENDMENT**	Para 7.4	"IT security policies" replaced with "IT Security Policy".
h.	**DELETION**	Para 7.4	Reference to Appendix 1 deleted.
i.	**AMENDMENT**	Para 8 (Bullet point 1)	"CLT" amended to "GCLT".
j.	**DELETION**	Para 8 (Bullet point 4)	Reference to "Directorate" deleted.
k.	**AMENDMENT**	Para 8 (second para)	"CLT" amended to "GCLT".
l.	**AMENDMENT**	Para 9	Policy Review amended from "annually" to "as required but at least every 24 months".

Appendix 4 – Remote Working Policy Revisions

Policy Title: **Remote Working Policy** New Version: 4.0

Applicable to: Members: Y

Staff (permanent, temporary, placements): Y

Partners: Y

Revisions:

a.	**ADDITION**	Para 1	Added “Homeworking Policy”
b.	**AMENDMENT**	Para 2 Bullet 1	Replaced “Team Manager, Member and Support Services” with “Team Manager, People and Organisational Development”
c.	**ADDITION**	Para 3	Added “and/or Homeworking Policy”
d.	**ADDITION**	Para 5	Added “Tablet Computers” to the list of portable electronic devices.
e.	**DELETION**	Para 6	Deleted “(TBA)” after “Legal Responsibilities Policy”.
f.	**AMENDMENT**	Para 7	Replaced “Team Manager, Member and Support Services” with “Team Manager, People and Organisational Development”
g.	**ADDITION**	Para 7.1 Bullet 13	Added “and other IT policies listed at Para 7.5 which stipulate the acceptable use of Council IT equipment MUST be followed (i.e. not accessing illegal or pornographic websites etc.).”
h.	**ADDITION**	Para 7.2	Added “A homeworking risk assessment should be carried out and approved by the user’s manager.”
i.	**AMENDMENT**	Para 7.2	Policy title amended to read “Information Management and Protection Policy”.
j.	**AMENDMENT**	Para 7.5	List of codes and policies amended to reflect current version.
k.	**DELETION**	Para 9	Deleted in Toto.
l.	**AMENDMENT**	Paras 9 and 10	Renumbered
m.	**AMENDMENT**	Para 9	Policy review amended from 12 monthly to 24 monthly
o.	**AMENDMENT**	Para 10	List of references amended to reflect current items.

Appendix 5 - Information Policy Revision Sheet

Policy Title: **IT Access Policy** New Version: 2.0

Applicable to: Members: Y

Staff (permanent, temporary, placements): Y

Partners: Y

Revisions:

a.	**AMENDMENT**	Para 6	Completely revised to adopt a new password policy based on guidance recently issued by the Government. This new policy mandates that users devise a longer but simpler password which only has to be changed annually unless compromised.
b.	**AMENDMENT**	Para 7.2	Paragraph completely reworded to remove references to "Systems Access Forms" (these are now referred to as "requests for access") and to introduce a new policy that all access to Council ICT systems is initiated by the People and Organisational Development Team. This new policy also applies to access to Council IT systems by members. The paragraph also clarifies who is responsible for actions when an employee or member leaves the Council.
c.	**AMENDMENT**	Para 7.3 (bullet point 4)	"Systems Access Form signed" replaced by "request approved".
d.	**AMENDMENT**	Para 8	Paragraph amended to clarify difference in disciplinary procedures for Council employees and members.
e.	**DELETION**	Para 9	Deleted in Toto.