EAST RIDING OF YORKSHIRE COUNCIL

Data Protection Policy

Lead Directorate and service:	**Corporate Strategy and Commissioning Directorate Resource Strategy Service**
Effective Date:	**May 2012**
Date Reviewed:	**July 2015**
Date Due for Review:	**April 2018**
Contact Officer:	**Matthew Turner**
Contact Number:	**01482 391419**
Approved By:	**Cabinet**

1. Background

It is the East Riding of Yorkshire Council's obligation to ensure compliance with the Data Protection Act 1998. The Information Commissioner, who oversees compliance and promotes good practice, requires all organisations and individuals who process personal data to comply with the eight data protection principles of 'good information handling'.

These are:

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes
3. Personal data shall be adequate, relevant and not excessive
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data shall not be kept for longer than is necessary
6. Personal data shall be processed in accordance with the rights of data subjects, including the rights to access information (Subject Access Request)
7. Personal data will be kept in an appropriately controlled and secure environment
8. Transfers outside of the European Economic Area require adequate levels of protection

The Act also requires all organisations and individuals who process personal information to register with the Information Commissioner's Office. This process is called Notification. The Council and its elected members are required to review their notification on an annual basis.

Data Protection law and policy aims to ensure that individuals' rights and freedoms are protected. Using personal data to abuse discriminate or deny access to services is unlawful. The Council is committed to ensuring that the personal data that it holds is used fairly and lawfully and in a non- discriminatory manner.

This policy applies to all personal data held by the Council. It encompasses manual/paper records and personal data electronically processed including information gathered on CCTV systems, of whatever type and at whatever location, for use by, or on behalf of, the Council.

This policy will be reviewed on a biennial basis to ensure that it reflects changes to existing legislation, and any new legislation.

2. Definitions for the Purposes of this Policy

There are other policies which provide guidance regarding ICT security, manual and paper records and records management. For the purposes of this policy, the following definitions are in relation to Data Protection.

The Council has adopted the following definitions as set out by the Information Commissioner:

Data means information which:

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68[1], or
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Personal data means data which relate to a living individual who can be identified:

(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

[1] 68 Meaning of "accessible record".
(1) In this Act "accessible record" means—
(a) a health record as defined by subsection (2),
(b) an educational record as defined by Schedule 11, or
(c) an accessible public record as defined by Schedule 12.
(2) In subsection (1) (a) "health record" means any record which—
(a) consists of information relating to the physical or mental health or condition of an individual, and
(b) has been made by or on behalf of a health professional in connection with the care of that individual.

Sensitive personal data means personal data consisting of information as to:

(a) the racial or ethnic origin of the data subject,
(b) an individual's political opinions,
(c) an individual's religious beliefs or other beliefs of a similar nature,
(d) whether an individual is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation Act 1992),
(e) an individual's physical or mental health or condition,
(f) an individual's sexual life,
(g) the commission or alleged commission by an individual of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of any court in such proceedings.

Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data.

Data subject means an individual who is the subject of personal data.

Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Recipient, in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

Third party, in relation to personal data, means any person other than:
(a) the data subject,
(b) the data controller, or
(c) any data processor or other person authorised to process data for the data controller or processor.

3. Policy Statement

In order to operate efficiently, East Riding of Yorkshire Council has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

East Riding of Yorkshire Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it carries out business. The Council will ensure that it treats personal information lawfully and correctly.

To this end the Council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

4. Corporate Requirements

East Riding of Yorkshire is a data controller under the Data Protection Act 1998.

Directors are responsible for ensuring compliance with the Data Protection Act 1998 and this policy within their directorates.

Directors and Heads of Service are responsible for ensuring that the business areas they have responsibility for have processes and procedures in places that comply with the Data Protection Act 1998 and this policy. Directors and Heads of Service are responsible for ensuring that data cannot be accessed by unauthorised personnel and to ensure that data cannot be tampered with, lost or damaged.

Responsibility for managing Data Protection is delegated to the Council's Data Protection officer as recognised by the Information Governance Management Board. The Corporate Strategy and Performance Team are responsible for providing day to day advice and guidance to support the Council in complying with the Data Protection Act 1998 and this policy.

Each Directorate's Data Protection Link Officer shall promote good practice and assist their Director and Heads of Service in ensuring compliance with the Data Protection Act 1998. The nomination of such a person shall not release other members of staff from compliance with the Data Protection Act 1998 and this policy. For more details regarding the roles and responsibilities of the link officer, these can be found in the References section below.

All employees or contractors and elected members who hold or collect personal data are responsible for their own compliance with the Data Protection Act 1998 and must ensure that personal information is kept and processed in line with the Data Protection Act 1998 and this policy. Failure to do so may result in disciplinary action which could lead to dismissal. Any processing of sensitive personal data must comply with the principles set out in the Data Protection Act 1998 and in section one of this policy.

Within the definitions stated in Section 2, the Data Controllers are subject to notifying the Information Commissioner's Office in order to be placed on the published list of registered data controllers. These include:

- East Riding of Yorkshire Council
- East Riding of Yorkshire Youth Offending Service
- Electoral Registration Officer for the East Riding of Yorkshire Council
- All East Riding Schools (as separate entries)
- Ward Councillors

Please see the References section to access the live list.

As data controllers, schools are responsible for their own policies and procedures regarding compliance with the Data Protection Act 1998.

5. Policy Development including Consultation

This policy has been developed in accordance with the Corporate Policy Guidance Notes. The following people and groups were consulted in development of this policy:

Information Governance Management Board
Corporate Management Team
Senior Management Team
Health, Diversity and Information Group Manager
Senior Research Officer

6. Links with other Policies and Strategies

This policy links to other Council documents:

- Information Management Strategy
- ICT Security Policy
- Records Management Policy
- Corporate Risk Register
- Humber Information Sharing Charter
- Risk Management Strategy
- Whistle Blowing Policy

7. Access Rights by Individuals (Subject Access Requests)

An individual may request to see any data held about them, or information about the reasons it is kept and processed. This is called a Subject Access Request under the Data Protection Act 1998. The Council has a Data Protection Request (Subject Access Request) – Process Guidance, which sets out procedures for access to personal data.

8. Disclosure of Personal Information about third parties

Personal data must not be disclosed about a third party except in accordance with the Data Protection Act 1998. If it appears absolutely necessary to disclose information about a third party to a person requesting data advice must be sought from the Corporate Strategy and Performance Team.

9. Information Sharing

Before sharing personal information it is the responsibility of individual members of staff to ensure that they have the authority to do so and that the recipient is authorised to receive such information. Failure to do so could lead to action under the Council's disciplinary procedure (and, in exceptional circumstances, in criminal charges). There is a Humber Information Sharing Charter which should be referred to when considering sharing data. See section 6 for a link to this charter.

10. Key Business Processes

When designing new business processes (including forms which are designed for the collection of data) this policy must be considered.

When considering the specification, procurement and testing of new items of hardware and software, this policy must be applied in conjunction with the ICT Security Policy.

When changes or amendments are made to either of the two above points, Data Protection compliance must be reviewed and a Privacy Impact Assessment should be considered (in conjunction with the Corporate Strategy and Performance Team).

11. Data Quality, Integrity and Retention

In order to process personal information, the data controller must have the consent of the data subject (unless a valid exemption is being applied). This consent can be gained through the use of a fair processing notice, stipulating how their collected personal data will be used.

If an individual complains that the personal data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the information. In the meantime a caution should be marked on the person's file that there is a question mark over the accuracy.

Individuals can request the Council to stop processing data for example, if data is properly held for marketing purposes, an individual is entitled to require that this is ceased as soon as possible. The cessation must be confirmed in writing.

If data is held for any other purposes, an individual may request that processing ceases if it is causing them unwarranted harm or distress. This does not apply if they have given their consent, if the data is held in connection with a contract with the person, if the Council is fulfilling a legal requirement or if the person's vital interests are being protected. Valid written requests must be responded to in writing within 21 days.

Procedures should be in place in order to ensure that the personal data is accurate, and that wherever possible this record is kept up to date.

12. Exemptions

Part 4 of the Data Protection Act 1998 outlines exemptions from the Act. Exemptions (depending on the circumstances) exempt the Council from certain aspects of the Act, for example granting subject access, providing privacy notices and disclosing personal data to third parties. The Corporate Strategy and Performance Team should be contacted in such circumstances who will, if required, make a decision in conjunction with the Senior Information Risk Officer and Caldicott Guardian.

13. Risk Management

Each service area is required to assess the level of information risk, in conjunction with the Data Protection Act 1998. This should be recorded in their Service Plan.

The requirement to maintain relevant risk is set out by the Risk Management Strategy, which has a primary focus towards business risk. When establishing the information risk, this should be cross-referenced with the Risk Management Strategy to ensure that the same evaluation and assessment process is followed.

As part of the Council approach to risk management the following guidance must be adhered to by all staff:

- Handling Personal Data Guidance
- Data Protection Request (Subject Access Request) – Process Guidance
- Data Protection Breach – Process Guidance
- Redaction Guidance
- Clear Desk and Screen Guidance

14. Breaches

The Council will always treat any data breach as a serious issue. In the event of a breach, or suspected breach, the Data Protection Co-ordinator should be informed immediately. If it involves IT then it must also be immediately reported to ICT. In conjunction with Legal Services, it will then be assessed whether the ICO should be notified. In addition the Head of HR must be informed to ensure appropriate investigation is undertaken in accordance with the Council's disciplinary policy. The Information Commissioner's Office has the authority to sanction significant financial penalties, of up to £500,000 in relation to breaches of any of the data protection principles.

The Council has a Data Protection Breach - Process Guidance, which sets out procedures to be followed in the event of any data breach or suspected breach. Any suspected data breach can also be raised anonymously through the Whistle Blowing Policy.

15. Training

It is the Council's policy that all employees and elected members who hold or process personal data receive the appropriate training in order to comply with the Data Protection Act 1998. Training in Data Protection matters should be provided before any access to personal data is permitted, and mandatory refresher training should be undertaken at intervals thereafter to maintain awareness. All new employees must complete the Induction Checklist, which includes a section on the Data Protection Act 1998. It is the responsibility of the managers of temporary or contracted staff to ensure they are aware of this Data Protection policy and their responsibility to adhere to it.

Data Protection training is a crucial element of staff awareness. All individuals need to be aware of their obligations relating to any personal data they process as part of their Council duties. Failure to adhere to the eight data protection principles can lead to serious misconduct and prosecution. All staff complete an e-learning package on Data Protection and those staff who handle personal data as part of their role attend face to face training.

16. Complaints

An individual has the right to complain about the response they have received regarding their request for information as well as to complain about other breaches of the Data Protection Act 1998. Details of the complaints procedure can be found in the References section below.

17. Outcomes and impacts

- Minimise the inappropriate use of personal data held on Council systems.
- Services and employees are aware of their responsibilities for handling personal data and that failure to do so could result in disciplinary proceedings.
- Service areas, employees and members are aware of their duties under the Data Protection Act 1998, and who to contact for advice.
- Service areas and group offices identify training requirements in association with handling personal data.
- Requests for personal data are handled in accordance with the Data Protection Policy.
- Third party data processors working on behalf of the authority will handle personal data in accordance with the Data Protection Policy.
- The Corporate Strategy and Performance Team is made aware of all and will formally log Data Protection Act 1998 breaches and their outcomes, and will inform the ICO as appropriate.
- The organisation is compliant with the Data Protection Act 1998.

18. Policy Implementation

The Data Protection Policy will be implemented through:

- Information Governance Management Group
- Senior Management Team
- Corporate Management Team
- Cabinet

19. Evaluation

The Data Protection Policy will be subject to a biennial review to ensure that it is appropriate and responsive to all relevant legislation and guidance.

20. References

Data Protection Act 1998
ICO website
ICO website – Data Controllers List
East Riding Data Protection webpage
East Riding Data Protection webpage – Guidance for elective and prospective members
Data Protection Link Officer – Roles and Responsibilities
East Riding Freedom of Information webpage
East Riding Complaints
East Riding Learning and Development
East Riding Information Management Strategy