Data Protection Policy

Adopted May 2015 by:-

Middlewich Primary School

Reviewed autumn term 2016

This policy is written in accordance with Cheshire East Council's Data Protection guidance.

Document Control

Organisation	Cheshire East Council
Title	CEC Policy
Author	Julie Gibbs
Subject	Data Protection Policy
Protective Marking	Not Protectively Marked
Review date	May 2015

Revision History

Revision Number	Revisor	Previous Version	Description of Revision	Date of Revision
0.01	LC	N/A	First draft	16.01.2012
0.02	JG	0.01	Second draft	29.02.2012
0.03	JG	0.02	Final draft	13.04.2012
0.04	JG	1	Amendments following Internal Audit	18.10.2013
0.05	JG	2	Amendments to reflect use of distribution lists	11.05.2015

Document Approvals

This document requires the following approvals:

Board/Committee/Group	Date
Corporate Governance Group	23.10.2013
SIRO Working Group	12.05.2015
Corporate Assurance Group	20.05.2015

Contents

1 Policy Statement

Cheshire East Council is committed to ensuring that the personal and sensitive personal information (data) it holds about individuals is used only for the purpose intended, is accurate, up to date and securely protected from inappropriate access. The Council is further committed to ensuring that individuals can find out about their personal data, be given access to it and the right to challenge its accuracy. In terms of non-personal information, the Council is further committed to promoting public access to the information it holds.

The Council supports the objectives of the Data Protection Act 1998. This policy is intended to maintain the confidentiality of personal data held or processed either on computer or in manual files and to increase the access given to individuals to information relating to them.

1.1. Registration/Notification

The Council has a notification with the Information Commissioner, registration number Z1543115. The Superintendent Registrar (Z1693267) and the Electoral Registrar (Z1693253) are also registered with the Information Commissioner separately.

1.2. Amount of data to be held

The Council will hold the minimum personal data necessary to enable it to perform its functions and retained in accordance with the Council's retention guidelines. Every effort will be made to ensure that data is accurate and up-to-date, and that inaccuracies are corrected quickly.

1.3. Subject Access

Upon written request, the Council will provide to any individual a reply stating whether or not the Council holds personal data about that individual. A copy of information held will be provided, in permanent form, subject to any exemptions as laid down in the Data Protection Act. A fee of £10 will be charged for this service, although the fee may be waived in certain limited circumstances. The Council will respond to this request as soon as possible and always within 40 calendar days.

1.4. Public Registers

The Council maintains a number of public registers that contain personal data or data that could be used to identify individuals. These are set out in Appendix 1. Strict compliance with the legislation giving rights of access to this personal data will be used in all cases. The Council's guiding principle will be to ensure that the data is only used for the purposes intended and understood by the individual(s).

1.5. Disclosures

Disclosures of information must be, and will be, dealt with in accordance with the provisions of the Act and the Council's notification. The Council has a duty to disclose certain data to public authorities such as HM Revenue and Customs and this will be done strictly in accordance with the statutory requirements.

Requests for disclosure of personal information, for example from the police for criminal investigations or solicitors for legal proceedings, must be made in writing. These requests will be logged by Compliance & Customer Relations and disclosure will only be granted if it is considered necessary for their purpose.

Where disclosures of personal data are made to distribution lists, these lists must be approved by a relevant Senior Manager or Head of Service. Recipients must be deemed appropriate to receive such information and lists must be reviewed and updated regularly (an appropriate recipient is one that has a clear and lawful business need to access such information). If distribution lists are not kept up to date, inappropriate disclosure could result in a breach of the Data Protection Act 1998 and cause reputational and financial damage to the council.

Disclosures will be communicated by secure means using only approved methods of transfer, for example one of the secure email solutions available. For further information and advice about secure transfer see CEntranet or contact icteastsecurity@cheshireeast.gov.uk.

Emails sent to external distribution lists must be sent using the "Bcc" field. This will avoid disclosing third party email addresses to other recipients.

1.6. System Design

The Council will ensure that personal data is treated as confidential. Computer systems will be designed and used to comply with the principles of the Data Protection Act so as to ensure that access to personal data is restricted to identifiable system users.

1.7. Training

It is the aim of the Council that all staff will be properly trained, fully informed of their obligations under the Data Protection Act and aware of their personal liabilities. Data Protection training is mandatory and forms part of the personal development review process.

1.8. Disciplinary Action

The Council expects all of its staff and members to comply fully with this Policy and the principles of the Data Protection legislation. Disciplinary action may be taken against any employee or member who breaches any of the instructions or procedures following from this policy.

2 Purpose

This document sets out Cheshire East Council's policy regarding data protection. The Data Protection Act 1998 is the basis of this document. The Freedom of Information Act 2000 affects the Council's use of non-personal information and the operation of this policy. The Human Rights Act 1998 affects the protection and individual rights given under the Data Protection legislation.

The purpose of the data protection legislation is to regulate the way that personal information about living individuals, whether held on computer or in a manual filing system, is obtained, stored, used, disclosed and destroyed. The legislation grants rights to individuals to see the data stored about them and to require modification of the data if it is wrong. In certain cases, individuals may claim compensation if they have suffered substantial damage as a result of the Council processing inaccurate data.

The 1998 Act requires all processing of personal data to be notified to the Information Commissioner and to be kept and used in accordance with the provisions of the Act.

3 Scope

This Data Protection Policy applies to all the systems, people and business processes that make up the Council's information systems. This includes all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Cheshire East Council purposes.

It applies to all information held in any format about living individuals, including personal data, sensitive personal data and financial data. This data will include details of, but is not restricted to:

- Current, past and prospective employees, including temporary and casual workers
- Elected members
- Suppliers
- Customers and clients
- Complainants, correspondents and enquirers
- Relatives, guardians and associates of the data subject
- School pupils and students
- Others with whom the Council communicates

4 Definition

This policy should be applied whenever a user accesses Cheshire East Council information systems or data in any form.

To aid the understanding of this document and provisions of the Data Protection Act the following definitions are provided:

Data is information that:

a) Is being processed by means of equipment operating automatically in response to instructions given for that purpose e.g. payroll system
b) Is recorded with the intention that it should be processed by means of such equipment e.g. on disk or CD ROM
c) Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system e.g. any departmental filing system with an index
d) Does not fall within paragraphs (a), (b) or (c) but forms part of an accessible record, e.g. health, education, public records
e) Is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)

Data Controller means the Council as the organisation who determines how data is processed.

Data Processor means any person, other than an employee of the Council, who processes data on behalf of the data controller, e.g. someone contracted to the Council to print documents containing personal data.

Data Subject is the individual about whom personal data is held.

Personal Data means data about a living individual who can be identified from that information (or from that and other information in the possession of the data controller). This includes an expression of opinion about the individual, but not any indication of the intentions of the data controller or any other in respect of that individual.

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

- Racial or ethnic origin of the data subject
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Criminal convictions

Processing is very widely drawn and means anything from obtaining, holding and using the information to disclosure or destruction of the information.

Special Purposes means any one or more of the following i.e. journalistic, artistic or literary.

Relevant Filing System is any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

5 Risks

Non-compliance could have a significant effect on the efficient operation of the Council and

may result in financial loss and an inability to provide necessary services to our customers. A financial penalty of up to £500,000 could be imposed by the Information Commissioner for a serious breach of the Data Protection Act 1998. Additionally, data loss could have an impact on citizens, whether as a group or individually, or cause reputational damage to the Council.

6 Principles

The Data Protection Act 1998 contains 8 governing Principles relating to the collection, use, processing and disclosure of data, and the rights of data subjects to have access to personal data concerning them. These Principles are:

1 Personal data shall be processed fairly and lawfully and, in particular shall not be processed unless at least one of the conditions in Schedule 2 is met. These can be summarised as consent, contract, legal obligation, vital interests, public interest and balance of interest. In the case of sensitive personal data at least one of the conditions in Schedule 3 must also be met which can be summarised as explicit consent, employment law, vital interests, non-profit associations, manifestly made public, legal claims, justice/statute of the Crown, medical purposes, ethnic monitoring.

2 Personal data shall be obtained only for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

6 Personal data shall be processed in accordance with the rights of the data subject under this act (this includes the rights of subjects to access the data and to correct it).

7 Appropriate technical and organisational measures shall be put in place to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (this relates to data security).

8 Personal data shall not be transferred to a country outside the European Economic Area unless that country ensures an adequate level of protection in relation to the processing of personal data.

These principles are regarded as the minimum standards of practice for any organisation with respect to personal data.

7 Responsibilities

7.1. The Council

Overall responsibility for the efficient administration of the Data Protection legislation lies with the Council.

7.2. Cabinet, Portfolio Holders, Directors and Heads of Service

Day to day responsibility for administration and compliance with the Act is delegated from the Council through the Cabinet, Portfolio Holders and Directors to respective Heads of Service for their service area. Within each service, a co-ordinator will be identified to assist in compliance with the requirements of the legislation on behalf of the department/service.

7.3 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is a Corporate Leadership Board member who takes overall ownership of the council's information risk management policy, acts as an advocate for information risk at board level and makes the annual statement of internal control of information risk.

Specific responsibilities include:

- Owns the Information Assurance policy (MS Word, 136KB)
- Provides a focal point for managing information risks and incidents including
    - Process for information risk assessment
    - Review and agreement of information risk mitigating actions
    - Discussion and resolution of information assurance issues
- Fosters a culture for the security and protection of information alongside the requirements for open and transparent communications
- Promotes the assurance of all information assets held by the organisation and its partners on its behalf.
- Keeps the Corporate Leadership Board and Cabinet informed of information assurance issues.

7.4 Data Protection Officer

It is the responsibility of the Data Protection Officer to assist the Council to ensure compliance with this policy and to specify the procedures to be adopted.

The main duties of the Data Protection Officer are:

- Provide advice and guidance to officers and elected members with regard to application of the Data Protection legislation
- Maintenance of the Council's notification under the Act, and act as an interface with the Information Commissioner
- Development, updating and publication of data protection procedures for the Council

- Initial contact point for subject access requests and requests for disclosure of personal data from other agencies

- In conjunction with HR Workforce Development, the provision of education and training regarding data protection issues

7.5. ICT Security

The duties of ICT Security include:

- Developing, maintaining and advising on compliance with the ICT Security Policies for both officers and members.

7.6. Departmental Co-ordinators

Existing departmental co-ordinators of freedom of information requests and corporate complaints will be responsible for:

- Liaising with the Data Protection Officer on all matters concerning administration of the Act within their department or service

- To work with senior management to ensure compliance with the legislation within their department or service

- Assisting in the co-ordination and response to subject access requests from individuals and requests for disclosure of personal data from other agencies

7.7. Officers and Elected Members

In addition to the formal responsibilities outlined above, all officers and members have a duty to observe the principles of the Act and the procedures referred to in this document.

Individuals who do not handle personal data as part of their normal work have a responsibility to ensure that any personal data they see or hear goes no further. This includes personal data and information extracted from such data, thus, for example, unauthorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or even inadvertently by reading a computer screen.

Elected members will be supplied with personal and sensitive data to enable them to fulfil their duties as ward councillors and members of cabinet or committees etc. Members must protect this data and prevent unauthorised or inadvertent disclosure of this data. In terms of data accessed by computer the ICT Security Policies will apply.

Disciplinary action may result if the Data Protection Principles or procedures outlined in this document are breached.

Elected members are similar to employees when handling personal data supplied to them by the Council. In such cases they are not considered to be Data Controllers and have no need to notify the Information Commissioner. However, elected members may hold structured manual or computer files of personal information obtained from other sources. These may

include constituent service requests and canvassing lists etc. In such cases the elected member will become a data controller and will need to notify the Information Commissioner.

Training and guidance will be provided for elected members in relation to their obligations under the Act. The Data Protection Officer will arrange registration of elected members with the Information Commissioner on their behalf.

8 Policy Compliance

If any user is found to have breached this policy, they may be subject to Cheshire East Council's Disciplinary or Dignity at Work Policies. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager.

9 Policy Governance

The following table identifies who within Cheshire East Council is Accountable, Responsible, Applicable or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted during final policy development.
- **Applies to** – the person(s) or groups that this policy is applicable.

Responsible	Data Protection Officer
Accountable	Customer Relations and Compliance Manager
Consulted	Corporate Assurance Group
Applies to	Elected Members, Council Employees, Temporary Staff, Contractors etc.

10 Review and Revision

This policy will be reviewed as it is deemed appropriate by the Corporate Assurance Group, but no less frequently than every 2 years.

11 References

The following Cheshire East Council policy documents are relevant to this policy:

- ICT Access Policy
- ICT Communications and Operations Policy
- ICT Computer, Telephone and Desk Use Policy
- ICT Flexible and Mobile Device Policy
- ICT Legal Responsibilities for Data Policy
- ICT Mail and Messaging Policy
- ICT Personnel Standards for Information Security
- ICT Internet Policy
- ICT Software Policy
- ICT Incident Management Policy
- Protective Marking Policy
- Paper Records – Secure Handling and Transit Policy

Additionally, details of the period of retention for information can be found in the following document:

- Retention Guidelines – Non Schools

A1 Appendix 1

List of Publicly available information that could be used to identify individuals

A1.1 Elections

Representation of the Peoples Act 1983

Register of persons who are eligible to vote in elections

Returns or declarations and accompanying documents relating to election expenses sent by a candidate of a parliamentary or local government election to the Council.

A1.2 Pecuniary Interests

Local Authority (Members' Interests) Regulations 1992

A register setting out the information which elected members give on their direct and indirect pecuniary interests.

A1.3 Members Allowances

The Local Authority (Members' Allowances) Regulations 1991

Records of payments made to elected members are open to inspection by local government electors for the area. Additionally, the authority must publish within its own area details of the total sums paid under the scheme.

A1.4 Committee Minutes, Reports, Forward Plan and Register of Key Decisions

Local Government Act 1972

Local Government 2000

Allows access to agendas and reports of committees and sub-committees. Minutes are also available.

A1.5 Taxis and Private Hire Vehicles

Town Police Clauses Act 1847

Local Government (Miscellaneous Provisions) Act 1976

Register containing information about owners and drivers of taxis and drivers of private hire vehicles.

A1.6 Charities

Charities Act 1993

An index that contains such information as the names of the trustees, the purpose of the charity and the accounts of the charity.