Data Protection Policy

Document Overview			
This data protection policy sets out the Council's commitment to protecting personal data and how this commitment will be implemented with regards to the collection and use of personal data.			
Intended Audience		All employees and Councillors	
Linked Policy		Information Governance Policy Information Sharing Policy Information Security Policy Records Management Policy Electronic Communications Policy	
Revision History			
Version	Author	Reason for issue	Date
1.0	Katy Deacon	Reviewed Policy	13/01/2017
Date of next revision		January 2018	

Policy Scope

This policy applies to

- all substantive and temporary employees of Kirklees Council
- any individual including contractors, volunteers and others who may have access to council data
- all work experience and other students
- elected members

This policy outlines the behaviours and responsibilities expected in order to ensure the council continues to fulfil its obligations under the Data Protection Act 1998.

Policy Statement

All staff and councillors at Kirklees Council are committed to:

1. ensuring that we comply with the eight data protection principles, as listed below
2. meeting our legal obligations as laid down by the Data Protection Act 1998
3. ensuring that data is collected and used fairly and lawfully
4. processing personal data only in order to meet our operational needs or fulfil legal requirements
5. taking steps to ensure that personal data is up to date and accurate
6. establishing appropriate retention periods for personal data
7. ensuring that data subjects' rights can be appropriately exercised
8. providing adequate security measures to protect personal data
9. ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues
10. ensuring that all staff are made aware of good practice in data protection
11. providing adequate training for all staff responsible for personal data
12. ensuring that everyone handling personal data knows where to find further guidance
13. ensuring that queries about data protection, internal and external to the organisation, is dealt with effectively and promptly
14. regularly reviewing data protection procedures and guidelines within the organisation

Roles and Accountability

The Council's Directors have responsibility for:

- ensuring the Authority's compliance with the Data Protection Act
- assigning responsibilities for adherence to the Authority's policies and procedures
- advising Elected Members on all matters relating to Data Protection within the Authority
- ensuring that complaints from the public or from the Information Commissioner's Office are dealt with promptly and appropriately.

All staff with line management or supervisory responsibilities are responsible for ensuring that staff under their control who process personal data in any way:

a. are made aware of their personal obligations and responsibilities under the Data Protection Act
b. receive appropriate training
c. are made aware of the Authority's policies and procedures relating to personal information

All individuals who have access to Council data are responsible for:

d. **c**omplying with the policy and legislation
e. ensuring good Information Governance practices are followed at all times
f. seeking advice, assistance and training when required

Associated Documents/Further Reading

This policy should be read in conjunction with the Appendix to all Information Governance related policies and the IG policies identified above.

Notes to the Data Protection Policy

Personal data is information about identifiable living individuals.

The Data Subject is the person whose data is processed by the Data Controller.
Processing includes anything done with data between (and including) collection to destruction.

The Data Controller: Kirklees Council, the Electoral Registration Officer, the Superintendent Registrar, the Youth Offending Team Manager, the Returning Officer and individual Councillors are separate Data Controllers for the purposes of the Act.

Data Subject Notice: a written notice from a Data Subject requiring the Data Controller to cease (or not begin) processing data about that individual which is, or is likely to be, harmful or distressing. A written response must be given within 21 days stating the agreement to comply, the intention to comply or the reasons why it is not appropriate to comply.