

To: City Executive Board

Date: 17 December 2014

Report of: Head of Business Improvement and Technology

Title of Report: Data Protection Policy Refresh

Summary and Recommendations

Purpose of report: To inform the City Executive Board of proposed minor changes to the current Data Protection Policy to keep it in line with best practice and new guidance issued by the Information Commissioner.

Key decision: Yes

Executive Lead Member: Cllr Turner, Executive member for Finance, Asset Management and Public Health

Policy Framework: No

Recommendations: That the City Executive Board endorse the amendments to the Data Protection Policy. The changes will be communicated to all staff with training provided as required. The information will also be updated on our intranet and website, online forms and all other relevant documents.

Appendix

Appendix 1: Updated Data Protection Policy

Background

1. Last year, the Council's Data Protection Policy was updated and approved.
2. Since implementing the new policy, all services have been offered face to face Data Protection training. An introduction to Data Protection is also part of the Council's bi-monthly induction event. A compulsory Data Protection e-learning module is currently being rolled out to all relevant staff.

3. The new e-learning module explains the requirement and responsibilities of all staff handling personal data in order to remain compliant with the Data Protection Act 1998.
4. The purpose of regular reviews and updating of the Data Protection Policy is to ensure that the Council keeps its policy fit for purpose and reflect current legislation and best practice.

Data Protection Policy changes

5. The changes include:
 - Clarification of the arrangements which need to be in place to facilitate data sharing with external partners and other relevant agencies (Objective 2)
 - Insertion of an additional policy objective for occasions when the Council uses a data processor. Where the Council instructs a third party to process data on the Council's behalf, the Council must ensure that suitable security arrangements are in place to protect personal data as the Council remains responsible for the data (Objective 3)
 - The current policy states that any new systems being implemented should undergo a privacy impact assessment. The proposed new wording has been changed to include projects as well as new systems (Objective 10)

Environmental and Equalities Impact:

6. The updated policy has no climate change or environmental impact.
7. The updated policy has no direct equalities impact and training and guidance will be available to all staff and councillors.

Financial Implications

8. The risk of not complying with the Data Protection Act could result in a fine of up to £500,000 for each data breach. The risk associated with this and the ongoing mitigating activities is updated on the corporate and service risk register each month.

Legal Implications

9. The updated policy has been reviewed in conjunction with the Head of Law and Governance. Any breach of the Act could result in enforcement action by the Information Commissioner.

Name and Contact details of author:

Name:	Lucy Neville
Job Title:	Information Management and Compliance Specialist
Contact details:	Tel : 01865 252068; e-mail : ineville@oxford.gov.uk

Appendix 1: Updated Data Protection Policy

Data Protection

Policy	Data Protection
Process / Guidance	N/A
Purpose To ensure that Oxford City Council complies with the Data Protection Act 1998	

Version Control

Version	Status	Date	Author	Comments
1.0	Approved	26 Apr '13	Lucy Neville	
2.0	Draft	October 2014	Lucy Neville	

Data Protection Policy

Statement of Commitment

Oxford City Council understands the importance of ensuring that personal data, including sensitive personal data is always treated lawfully and appropriately and that the rights of individuals are upheld.

Oxford City Council is required to collect, use and hold personal data about individuals. Data is required for the purposes of carrying out our statutory obligations, delivering services and meeting the needs of individuals that we deal with. This includes current, past and prospective employees, service users, members of the public, Members of the Council, our business partners and other local authorities or public bodies.

Policy Objectives

In order to comply with the requirements of the Data Protection Act 1998, we will ensure that:

1. Any personal data will be collected, used and held, lawfully and appropriately.
2. Regular data sharing with external partners and other relevant agencies will be subject to information sharing agreements. Partnerships will only be entered into where there is a clear statutory power enabling the council to participate such as the Crime and Disorder Act 1998.
3. External agencies contracted to undertake any data processing on behalf of the City council will be required to demonstrate compliance with the Data Protection Act and satisfy the council that it has the necessary technical and organisational measures in place to protect personal data.
4. There are policies and procedures in place which are regularly reviewed and updated to ensure staff understand their responsibilities towards protecting personal data.
5. Training needs are identified and provided to ensure that those handling personal data are trained appropriately.
6. There is an appointed officer within the organisation who has specific responsibility and knowledge about data protection compliance covering all aspects within the scope of this policy and who is a point of contact for all queries.
7. There are a number of employees throughout the organisation who have specific responsibilities for data protection.

8. Data Subjects rights can be fully exercised.
9. Subject Access Requests are dealt with promptly and courteously.
10. Any new projects being implemented that involve personal data will undergo a privacy impact assessment.
11. The Council will regularly review and update this policy, procedures and guidance for Council employees and Members.

The Council is required by law to share or make available some of the personal data it collects and holds. This information may be shared for a number of reasons including to safeguard public funds and for the prevention and detection of fraud, and for the prevention and detection of crime. For more details on this please read Oxford City Council's [Privacy Notice](#)¹.

Oxford City Council is fully committed to compliance with the requirements of the [Data Protection Act 1998](#) and is registered as a data controller with the [Information Commissioner's Office](#). Our registration number is **Z7925628**.

Meeting our Policy's Objectives

In order to meet the objectives that are listed above Oxford City Council needs to ensure that the following are always considered and that appropriate controls and procedures are in place to ensure compliance with the Data Protection Act.

Collecting and Processing Personal Data

- When we collect personal data we will ensure that where required, we make individuals aware that their information is being collected, the purpose for collecting the data specified, and whether it will be shared with any third parties. This will be done through the use of privacy notices. When reviewing documents and forms, we will always consider whether a privacy notice should be included.
- No new purpose for processing data will take place until the Information Commissioner's Office has been notified of the relevant new purpose and the data subjects have been informed and consent has been sought where required.

¹ Please see <http://www.oxford.gov.uk/privacy> for Oxford City Council's Privacy Notice

Data Security

- Council employees and Members must report any suspected data breaches to the Data Protection Officer for investigation and where necessary the Data Protection Officer will notify the Information Commissioner's Office
- Council employees and Members must use appropriate levels of security to store or share personal data. Corporate guidance will be published and training will be provided to employees and Members
- When new projects involving personal data are being developed, Privacy Impact Assessments will be carried out by the Project Manager and reviewed by the Data Protection Officer in order to assess any privacy risks.

An Information Asset Register will be maintained by the Data Protection Officer identifying:

- all personal data held
- where it is held
- how it is processed
- what teams have access to it
- who has overall responsibility for the data.

Personal data will not be shared with a third party organisation without a valid business reason and where required Oxford City Council will notify individuals that the sharing will take place in the form of a privacy notice. If any new purposes for the data sharing are to take place, we will seek consent from the individuals concerned.

When personal data is to be shared regularly with a third party, a Data Sharing Agreement must be implemented.

Any data sharing will also take into consideration:

- any statutory basis of the proposed information sharing
- whether the sharing is justified
- how to ensure the security of the information being shared.

Data Access

- Council employees and Members will have access to personal data only where it is required in order to fulfil their role.
- All data subjects have a right of access to their own personal data; employees will be made aware of and will provide advice to data subjects about how to request or access their personal data held by Oxford City Council. More information is available on our [Subject Access Requests page](#)
- Council employees and Members are aware of what to do when requests for information are made under the Data Protection Act.
- Employees and Members are made aware that in the event of a Subject Access Request being received by Oxford City Council, their emails may be searched and relevant content disclosed.
- Privacy Notices will include a contact address for data subjects to use should they wish to submit a Subject Access Request, make a comment or complaint about how Oxford City Council is processing their data, or about the handling of a Subject Access Request.
- A Subject Access Request will be acknowledged to the data subject within three working days, with the final response and disclosure of information (subject to exemptions) within 40 calendar days.
- A data subject's personal data will not be disclosed to them until their identity has been verified and a fee of £10 has been paid.

- Third party personal data will not be released by Oxford City Council when responding to a Subject Access Request (unless consent is obtained, it is required to be released by law, or it is deemed reasonable to release).

Compliance with this Policy

- This Policy applies to all Oxford City Council employees, Council Members and all people or organisations acting on behalf of the Council.
- Each Head of Service/Director shall ensure compliance with this policy appropriate to the personal data activities within their remit.
- If any Council employee, or Member or persons acting on the Council's behalf are found to knowingly or recklessly breach the Council's Data Protection Policy appropriate disciplinary and/or legal action will be taken.
- The Council has a designated Data Protection Officer and designated officers with data protection responsibilities have been identified in all service areas.

Implementation of this policy will be led by the Council's Data Protection Officer.

Any questions or concerns about this policy should be taken up with the Council's Data Protection Officer

Data Protection Officer

Oxford City Council

Town Hall

St Aldate's

Oxford

Dataprotection@oxford.gov.uk

01865 249841

This page is intentionally left blank