www.oxford.gov.uk
OXFORD CITY COUNCIL

To: **City Executive Board**

Date: **12th June 2013**

Report of: **The Head of Business Improvement & Technology**

Title of Report: **APPROVAL OF A NEW DATA PROTECTION POLICY**

Summary and Recommendations

Purpose of report: To seek the approval of the City Executive Board for a new Data Protection Policy to reflect the Data protection Act amendments in 2008.

Key decision Yes

Executive lead member: Cllr. Ed Turner

Policy Framework: No

Recommendation(s): City Executive Board is asked to approve the Data Protection Policy and to note the new Data Protection guidance framework.

Appendices to report

Appendix 1. Data Protection Policy

Appendix 2: Data Protection guidance framework

Background

1. The Council's current Data Protection Policy is over 9 years old and does reflect the legislative updates, current best practice, and does not provide any supporting officer guidance.

2. The Data Protection Act amendment of 2008 gave the Information Commissioner's office (ICO) new powers to impose significant fines of up to £500,000 on bodies found in breach of the Data Protection Act.

3. The purpose of rewriting the Data Protection Policy is therefore is to ensure that the Council has a policy that is fit for purpose and effectively reflects current legislation and best practice. This review has also involved preparing a new framework of supporting guidance and training for Councillors and Officers.

New Data Protection Policy

4. The new policy includes how, in practical terms, the Council will comply with the Data Protection Act.
5. The new policy sets out the standards that the Council will work to in relation to processing personal data and safeguarding the rights of individuals.
6. Technological progress has profoundly changed the way our data is collected, accessed and used. The Policy aims to address these issues.
7. The new policy explains the Council's approach to embedding good data protection practices into the framework of the Council. This will be achieved as set out in the following section.
8. The new Policy is clear and concise, and it is hoped that it can be easily understood by all. The new policy, guidance and training that aims to interpret the technical aspects of the Data Protection Act into a way that is meaningful for staff.
9. The new policy continues to charge £10 for responding to a Subject Access request. This amount is set by the Information Commissioner and is the maximum amount we are allowed to charge.

Officer and Councillor Guidance and Training

10. In conjunction with the development of the new policy a considerable amount of work has gone into creating new standards and guidelines for councillors and officers relating to the specific Data protection issues they face in their day to day work when handling or processing data. The relationship between the Policy and the standards and guidelines is shown in the guidance framework at Appendix 1.
11. The new framework will be available on the intranet and under each heading there will be user guidance and templates for use by staff.
12. A suite of new data protection training courses will be available from the end of June 2013 using the Council's iLearn tool. Induction training now includes a section dedicated to data protection, and team training sessions have already been provided to areas where there is regular communications with customers.
13. Effective training and communication to all relevant staff is fundamental to ensuring the Council is able to demonstrate that it has robust arrangements in place to ensure officers and councillors are aware of their responsibilities in the handling and sharing data and ensuring the Council complies with the Data Protection Act.

Environmental and Equalities Impact.

14. The new policy has no climate change or environmental impact.
15. The new policy has no direct equalities Impact and training and guidance will be available to all staff and councillors.

Financial Implications

16. There are no direct financial implications; however failure by the Council to adhere to the Data Protection Act requirements can result in a fine of up to £500,000 for each data breach.

Legal Implications:

17. The new policy has been developed in conjunction with the Head of Law and Governance and approved by him. A breach of the act could result in the Information Commissioner issuing enforcements, undertakings and imposing a large fine on the Council.

Name and Contact details of author:

Name	Gary Thomas
Job Title	Chief Technology Manager
Service Area / Department	Business Improvement and Technology
Contact details	Tel : 01865 252220; e-mail : gthomas@oxford.gov.uk

Appendix 1 : Proposed Data Protection Policy

Data Protection Policy

Statement of Commitment

1. 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.

2. 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

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

    - Any personal data will be collected, used and held, lawfully and appropriately.
    - There are policies and procedures in place which are regularly reviewed and updated to ensure staff understand their responsibilities towards protecting personal data.
    - Training needs are identified and provided to ensure that those handling personal data are trained appropriately.
    - 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.
    - There are a number of employees throughout the organisation who have specific responsibilities for data protection.
    - Data Subjects rights can be fully exercised.
    - Subject Access Requests are dealt with promptly and courteously.
    - Any new systems being implemented will undergo a privacy impact assessment.
    - A regular review and audit of the use of personal data is undertaken.
    - The Council will regularly review and update this policy, procedures and guidance for Council employees and Members.

4. The Council is required by law to share or make available some of the personal data it collects and holds. This information is shared 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].

5. 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.**

[1] Please see http://www.oxford.gov.uk/websitetools/privacy.cfm for Oxford City Council's Privacy Notice

Meeting our Policy's Objectives

6. 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

7. When we collect personal data we will ensure 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 which all documents and forms that collect personal data are required to include.
8. 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.

Data Security

9. 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
10. 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
11. When new systems are being developed, Privacy Impact Assessments will be carried out by the Project Manager and reviewed by the Data Protection Officer before devising system design in order to assess any privacy risks
12. An Information Asset Register will be maintained by the Data Protection Officer identifying:
    a. all personal data held
    b. where it is held
    c. how it is processed
    d. who has access to it
    e. who has overall responsibility for the data
13. Personal data in any format 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.
14. When personal data is to be shared with a third party, a Data Sharing Agreement will be implemented.
15. Any data sharing will also take into consideration:
    a. the statutory basis of the proposed information sharing
    b. whether the sharing is justified
    c. how to ensure the security of the information being shared.

Data Access

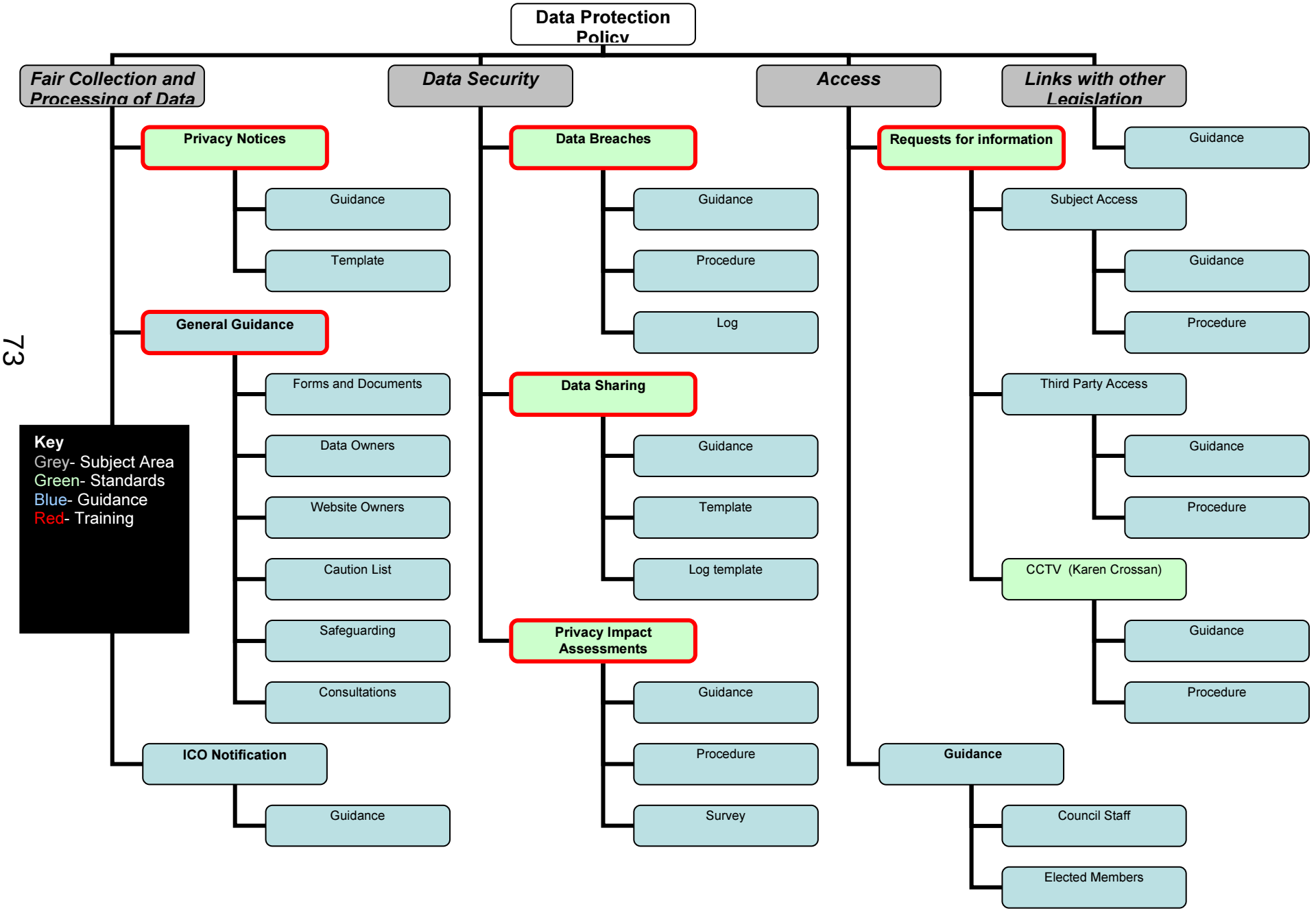
16. Council employees and Members will have access to personal data only where it is required in order to fulfil their role.
17. All data subjects have a right of access to their own personal data; employees will be made aware of and will provide advice to data subjects about how to request or access their personal data held by Oxford City Council.
18. Council employees and Members are aware of what to do when requests for information are made under the Data Protection Act
19. 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.
20. 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.
21. 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.
22. 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.
23. 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

24. This Policy applies to all Oxford City Council employees, councillors and all people or organisations acting on behalf of the Council.
25. Each Head of Service shall ensure compliance with this policy appropriate to the personal data activities within their remit.
26. If any Council employee 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. Councillors are expected to abide by their Code of Conduct.
27. The Council has a designated Data Protection Officer and designated officers with data protection responsibilities have been identified in all service areas/directorates.
28. Implementation of this policy will be led by the Council's Data Protection Officer.
29. 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
Oxford
Dataprotection@oxford.gov.uk
01865 249811

Appendix 2 - Data Protection guidance framework



This page is intentionally left blank