Data Sharing Policy

December 2018

Document Version	5.0
Document Status	Published
Owner Name	Caroline Parker
Owner Job Title	Information Services Manager
Document ref.	
Approval Date	06/12/2018
Review Date	18/09/2019

Data Sharing Policy

Document Control and Information

Status	Approval Date	Review Date
Published	06/12/2018	18/09/2018

Document Owner's Name	Job Title
Caroline Parker	Information Services Manager

Do not alter, copy, publish or distribute without the approval of the Document Owner

This instruction applies to:-

This policy applies to anyone needing access to Oxfordshire County Council's information systems, applications and equipment for their work in the office, at home, and elsewhere. This includes all temporary and permanent council staff, contractors, staff working under contract for external agencies commissioned by the council, volunteers and Councillors.

For Action by

As above.

For Information

As above.

Revision History

Version	Date	Author / Reviewer	Notes
5.0	06/12/2018	Information Management Team	Annual Review
4.0	18/04/2018	Information Management Team	GDPR/Annual Review
3.0	02/09/2016	Information Management Team	Annual Review.
2.0	26/08/2015	Information Management Team	Annual Review.
1.0	08/2014	Information Management Team	Minor revisions

Distribution and/or Publication

	Location	Date
All Staff	OCC Intranet	06/12/2018

Contents

1. Policy Statement

Oxfordshire County Council expects data generated by the council to be shared with as few restrictions as possible in a timely and responsible manner.

PLEASE NOTE: throughout this policy are links to other relevant policies and procedures. All users should take the time to familiarise themselves with all these documents.

2. Purpose

This policy does not replace existing data sharing agreements, providing that the principles of such agreements are consistent with those of this policy.

Information will be responsibly shared throughout the organisation. Where the council shares personal or sensitive data with partners and third parties on an on-going and systematic basis, it will enter into data sharing agreements before sharing such information.

The council recognises the importance of data quality, accuracy, timeliness and provenance. Wherever possible, data will be accompanied by contextual information or documentation (metadata). This metadata provides anybody using the data with details on the origin or manipulation of the data to help prevent misuse, misinterpretation or confusion.

3. Scope

This policy applies to anyone needing access to Oxfordshire County Council's ICT systems, applications and equipment for their work in the office, at home, and elsewhere. This includes all temporary and permanent Council staff, contractors, staff working under contract for external agencies commissioned by the Council, volunteers and Councillors.

4. Policy Compliance

Failure to comply with this policy may lead to disciplinary action. In the case of council employees this will be in accordance with the agreed disciplinary procedures and Officers Code of Conduct; for elected members it will be in accordance with the Code of Conduct for Members. For other groups the equivalent procedures and standards will apply.

It should also be noted that any information - including emails and attachments, texts, pictures and media posts - may need to be disclosed under the Data Protection Act 2018, General Data Protection Regulations and the Freedom of Information Act 2000.

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

5. Roles and Responsibilities

All users are required to accept and abide by the requirements of this policy and any associated procedures.

All managers are responsible for ensuring their staff abide by the requirements of this policy.

6. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Information Services Manager.

7. Data Sharing Procedure

Actions Before Sharing Data

Where the council shares personal or sensitive data with any third party on an on-going and systematic basis, you must enter into an Information Sharing Agreement before sharing such data. As a minimum any such agreement will document:

- The purpose, or purposes, of the data / information sharing.
- The potential recipients or types of recipient and the circumstances in which they will have access to the data/information.
- The data / information to be shared.
- Data / information quality standards.
- Data / information security arrangements.
- Arrangements for the retention of shared data.
- Retention & disposal including end of contract disposal.
- Individuals' rights – procedures for dealing with access requests, queries and complaints.
- Plans for the periodic review of effectiveness of the sharing agreement.
- Sanctions for failure to comply with the sharing agreement.
- How the agreement will be terminated and the return of council data.

Before any Information Sharing Agreement is entered into, you must check with Information Management Team to ensure it meets statutory requirements.

Please refer to the ICO's Data Sharing Checklist , below to help you decide whether your data should be subject to an Information Sharing Agreement.

Any person sending data utilising the ICO's Data Sharing Checklist should also conduct a proportionate risk assessment. As part of the assessment the Data Sender should consider the following points:

- Do not assume that because a Data Requester asks for information that they are entitled to receive it.
- Is the request to share data actually a Freedom of Information (FoI) request? Please refer to the FoI pages on the intranet. If you do not understand what your obligations are under this Act please speak to your line manager.
- Sharing of Personal Data and Sensitive Personal Data is subject to the Data Protection Act. Please refer to the Data Protection Act pages on the Intranet for guidance. If you do not understand what your obligations are under this Act please speak to your line manager.
- If your service area is not the owner of the information, you will need to obtain approval from the owner before sharing.
- Any requests to share information with media organisations should be referred in the first instance to the council's Media Team. Please refer to the Handling Media Enquiries page on the Intranet.
- Your team may have further procedures / requirements in place for sharing sensitive and / or personal data. If you have not seen these please consult your line manager.
- Is any of the data protectively marked? Please refer to the Security Classification Procedures for information on classifying and sharing protectively marked information.

Methods of Sharing Data

Email

Please refer to the council's Email Policy and Procedures for the correct method of sharing data and information by email.

Other Electronic Methods of Data Sharing

If you have a need to share data or information electronically other than by email you must contact the ICT Service Desk and obtain approval from the Information Management Team **before** the data or information is shared.

FAX

Do not share any sensitive or personal data by FAX unless there is **NO** other option. FAX is not a secure sharing method;

- FAX machines often save copies of received faxes internally; it may be possible for someone with access to print additional copies of that FAX.
- FAX machines generally print direct to paper; this may be left in an unsecured location.

Your team may have further procedures / requirements in place for sharing sensitive and / or personal data. If you have not seen these please consult your line manager.

Where possible have fax 'numbers' pre-set so reducing the risk of an error.

Postal Service or Hand Delivery

If you use the postal service for sending any sensitive data you should use secure postal services.

Your team may have further procedures / requirements in place for sharing sensitive and / or personal data. If you have not seen these please consult your line manager.

Telephone / Mobile Phone

As phone calls may be monitored, overheard or intercepted either deliberately or accidentally, it is advisable to share the minimum of information by telephone or mobile phone.

You must always be sure to establish the identity of the person you are speaking to and that they are entitled to have the information. If in doubt, **do not** share information with them.

Your team may have further procedures / requirements in place for sharing sensitive and / or personal data. If you have not seen these please consult your line manager.

Unacceptable Data Sharing

The following methods of sharing data outside the council are unacceptable and may result in disciplinary action and, where appropriate, criminal investigation:

- Sharing data via Internet Based collaborative sites or any other unsecure internet resource.

Sharing any sensitive or personal data through text messages or instant messages via any device.

8. Data Sharing Checklist.

1. Data Sharing Checklist - systematic data sharing

Before you enter into an agreement to share council data on an ongoing basis, consider the following:

a. Is the sharing justified?

Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

b. Do you have the power to share?

Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

c. If you decide to share

It is good practice to have a data sharing agreement in place.

As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

2. Data sharing checklist – one off requests

Before you share council data relating in 'one off' circumstances, consider the following:

a. Is the sharing justified?

Key points to consider:

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the DPA to share?

b. Do you have the power to share?

Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).

- Any legal obligation to share information (for example a statutory requirement or a court order).

c. If you decide to share

Key points to consider:

- What information do you need to share?
    - Only share what is necessary.
    - Distinguish fact from opinion.
- How should the information be shared?
    - Information must be shared securely.
    - Ensure you are giving information to the right person.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

d. Record your decision

Record your data sharing decision and your reasoning – whether or not you shared the information.

If you share information you should record:

- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Your justification for sharing.
- Whether the information was shared with or without consent.

End of document