ROYAL BOROUGH OF WINDSOR AND MAIDENHEAD

www.rbwm.gov.uk
Royal Borough of Windsor & Maidenhead

Security Policy

SECURE DATA TRANSFER TO OTHER ORGANISATIONS

Introduction

This policy defines the security procedure that must be completed before transfers of council owned data to or from other organisations. This should ensure that the appropriate level of protection is provided. A Data Transfer Agreement defines the purpose of the transfer, and states who is responsible both in the council and at the outside organisation.

Policy Statement

All data transfers of personal or sensitive information to outside organisations must be controlled. For once-off transfers, a Data Transfer Agreement must be created and the security precautions agreed. For regular data transfers (as part of an externally provided Service) a Service Level Agreement must be defined and included in the contract with the outside organisation.

Policy Aim and Benefits

Security risks during transfer of data are controlled through the policy and a transfer agreement. The benefits include a reduction in data loss or unauthorised disclosure. Also, there should be reduced costs of consequential damage. This includes damage to the council's reputation.

Not covered by this Policy

Transfers of unclassified data that can be made available to the public.

Those Affected

All council managers and those responsible for the transfer of data to outside organisations.
All outside organisations and third parties who may receive data from the council.

Roles and Responsibilities

1. Council managers and their staff - ensure a Data Transfer Agreement or Service Level Agreement is created and signed before any data is transferred.
2. Third Parties and Outside Organisations – cooperate in the creation and agreement of Data Transfer Agreements or Service Level Agreements.
3. Information Governance Team – provide advice and check compliance to agreements when required.

Policy Compliance

This policy must be complied with at all times, and any breach of the policy could constitute a disciplinary offence. If you do not understand the implications of this policy, or how it may apply to you, seek advice from your line manager, the IT Service, or from the Information Governance team.

Procedure

For once-off Data Transfers

1. The council manager must provide the outside organisation or third party with a copy of this policy and a blank Data Transfer Agreement.
2. Agree the detailed arrangements for secure transfer of the data concerned.
3. Document the arrangements in the Data Transfer Agreement.
4. Both parties sign and date the Agreement.
5. An electronic copy of the signed Data Transfer Agreement must be returned to the IT Service on ICTSecurity@rbwm.gov.uk
6. The data transfer may now take place.

For regular Data Transfers within a formal Contract

1. Agree the detailed security arrangements for these data transfers.
2. Document these arrangements within the contract as a Service Level Agreement.
3. The council manager is then responsible for compliance with the Service Level Agreement.

Related Policies

Storage of Information Policy
(which explains how to register any use of portable computer media for security purposes)
Use of Email Policy

Related Documents

Data Transfer Agreement

Related Legal and Regulatory Obligations

The UK Data Protection Act

Any Other Information

Note that any data transfers using email must use encryption security to reduce the risk of accidental disclosure of unprotected data on the Internet. Council personal or sensitive information must not be sent unprotected across the Internet.