Data Transfer Policy

London Borough of Barnet

(C) Copyright London Borough Barnet 2016

Document Control

POLICY NAME	Data Transfer Policy		
Document Description	Policy surrounding data transfers (electronic and paper based). This policy outlines the restrictions and necessary data security processes that must be followed when transferring data.		
Document Author 1) Team and 2) Officer and contact details	1) Information Management Team 2) Lucy Martin, lucy.martin@barnet.gov.uk ext: 2029		
Status (Live/ Draft/ Withdrawn)	Final	**Version**	03.00
Last Review Date	September 2015	**Next Review Due Date**	April 2017
Approval Chain:	Head of Information Management	**Date Approved**	April 2016

Version Control

Version no.	Date	Author	Reason for New Version
V.1	Dec 2010	Pattison Gbormittah	New Policy
V.1.2	Dec 2012	Lucy Wicks	Review – No change
V.2	Apr 2014	Lucy Martin / Dennis Hunt	Review
V3	September 2015	Lucy Martin / Dennis Hunt	Annual Review. Review needed to account for changes in law and internal process.

(C) Copyright London Borough of Barnet 2016

Contents

(C) Copyright London Borough Barnet 2016

1. Introduction

There are many occasions when transfer of council data is required between internal departments, third party service providers, public bodies, commercial organisations and individual officers to perform business functions.

It is essential that any transfer is done in a way that is appropriate for the type of data being transferred.

If the information is personal or sensitive personal data as defined by the Data Protection Act 1998 (DPA) or considered business confidential it is essential that the transfer is performed in a way that adequately protects the information. Throughout this policy, data of this nature is referred to as ‘controlled data’.

The DPA regulates the use of personal or sensitive personal information and lists 8 Principles that must be followed when handling personal data.

Data can potentially be transferred in a wide variety of media and methods both into and out of the council, in electronic and/or paper format. In every transfer there is a risk that the information may be lost, misappropriated or accidentally released. Where this data is controlled data, this represents a risk to the council of breaching our responsibilities under the DPA and could lead to regulatory action, including significant fines.

2. Purpose and scope

This policy lays out the practical methods that need to be applied in undertaking a transfer of data, and will provide additional guidance more specifically on the transfers of controlled data.

This policy is applicable to anyone handling council information that may have a need to transfer council data, including:

- employees of the council
- contractors
- agency staff
- Councillors handling council information
- contractual third party suppliers
- agents and partners of the council.

3. Initial considerations

Before you undertake a physical data transfer, ensure you have the appropriate authorisation to do so. Bear in mind any restrictions in place for the sharing or transfer of controlled data.

(C) Copyright London Borough Barnet 2016

- Never automatically assume someone is entitled to the information just because they have told you they need it, regardless of whether they are an internal or external requester.

- When dealing with third parties consider whether there are any data sharing agreements or contracts in place that cover the transfer of data. Check whether there are any stipulations in place regarding the method of transfer that should be used.

- Think about whether a non-disclosure agreement is required to cover security and use of the data.

- Check that you are not providing more information than is necessary for the identified purpose. Do not just send a whole document or spreadsheet because it is 'easier', when only one section or specific columns are required.

- Can the objective / purpose be met using anonymised data instead?

- Consider the most appropriate (not necessarily the easiest) transfer or access method.

- What risk does the transfer or access to information pose (if any)?

- For all transfers of information containing controlled data, it is essential that you appropriately establish the identity and authorisation of the recipient.

N.B. If you are you are in doubt you should seek further advice from the Information Management Team.

4. Data transfer methods

This section lists the main methods of data transfer and also sets out any restrictions and requirements for the secure transfer of controlled data.

Before choosing your method of transfer you must consider the following:

- the nature of the information, its sensitivity, confidentiality or possible value
- the size of the data being transferred
- the damage or distress that may be caused to individuals as a result of any loss during transfer
- the implications any loss would have for the council

You must only send information that is necessary for the stated purpose. You must remove any unnecessary data, and any data not required should be redacted or removed completely (as appropriate) before transfer.

(C) Copyright London Borough Barnet 2016

4.1. Via email

There are 3 main email routes that can be considered when transferring data via email. These are outlined below, with relevant restrictions highlighted.

All transfers of data by email must be done in a way that complies with the council's Acceptable Use Policy. As stated:

> *"Sensitive Personal Data (as defined by the Data Protection Act 1998) and highly confidential information when sent externally must only be sent via secure email such as GCSx or Encrypt and Send. Users are responsible for considering the sensitivity of data in an email before they send it and choosing the most appropriate method of transfer."*

General email rules

- Secure email should not be used for transfer of large amounts of data or significant numbers of records. The file size of an email is restricted to 30Mb, therefore, if you are sending large volumes of data that are likely to exceed your system's capacity, you should consider an alternative transfer method as explained in paragraph 4.5 below.

- Email messages must contain clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipient.

- Information sent must, where practical, be enclosed in an attachment.

- Be careful as to what information you place in the subject line of your email or in the accompanying message. Filename or subject line must not reveal the full contents of attachments or disclose any sensitive personal data.

4.2. Via standard email "@barnet.gov.uk"

When sending information internally between "barnet.gov.uk" addresses, this is already secure and does not require any additional actions, as the information being sent is not leaving the Barnet network.

However, using your Barnet account to send information to a non-Barnet address (i.e. something other than @barnet.gov.uk) over the open internet is not secure. This method of transfer should not be used to send any controlled data.

If you do need to apply an extra level of security for controlled data you can encrypt and apply a password to an email attachment. In Microsoft Office 2010, you can use passwords and encryption to help prevent other people from opening or modifying your documents, workbooks, and presentations. It's important to know that if you don't remember your password the missing password cannot be retrieved and therefore the file will not be accessible. Instructions on how to encrypt documents and construct passwords can be found using the Microsoft Help system.

(C) Copyright London Borough Barnet 2016

- All password(s) assigned to encrypted documents must conform to the minimum corporate Password Policy.

- All password(s) required to open the encrypted attached file must be transferred separately to the recipient either via a telephone call to an agreed number, or by SMS text message

- Be careful as to what information you place in the subject line of your email or in the accompanying message. Filename or subject line must not reveal the contents of the encrypted file.

- Note encryption is not required if the message is being sent internally on the @barnet.gov.uk domain.

4.3. GCSx email "@barnet.gcsx.gov.uk"

GCSx is an assured transport network between public bodies, local authorities, Health, Police, Criminal Justice and other PSN (Public Sector Network) connected organisations.

If you have a GCSx email account in Outlook you can send information securely by email without any additional security **providing** that the recipient also has an email address on an approved secure domain (pnn, NHS.net, CJSM etc.) email address. A GCSx account can be requested from IS self-service.

- GCSx email accounts must be used when sending sensitive personal data or information you consider to be highly confidential.

- Encryption or password protection of the document prior to transfer is not required if you are using GCSx because the network is inherently secure and encrypted files are blocked by the PSN infrastructure.

- The mail should be marked in accordance with the Government Security Classification (GSC) scheme which would normally be OFFICIAL OR OFFICIAL SENSITIVE (or similar sub-classification). Further information can be found in the council's Protective Marking Policy.

REMEMBER - GCSx email communications are only secure if both the recipient and the sender are a public body, local authorities, Health, Police, Criminal Justice and / or other PSN (Public Sector Network) connected organisation. Further guidance is available here.

4.4. Via encrypt and send

Encrypt and Send is the current council method of emailing information in a secure manner from a Barnet mail account, to an individual who does not have a GCSx account or is not on the PSN network.

(C) Copyright London Borough Barnet 2016

In the absence of the preferred GCSx, Encrypt and Send will protect the email content and attachment against unauthorised access.

Emails sent using Encrypt and Send are not sent directly to a recipient email address they are stored on a Secure Message Server which protects the sensitive information against unauthorised access. The recipient will need to undertake an initial registration to the message server site in order to be able to retrieve the message and respond. The information is accessed via the Web browser and the actions a user can perform are limited.

- Encrypt and Send should be used when:

  (a) sending sensitive business and sensitive personal information via email to an individual or organisation outside of the London Borough of Barnet's secure email network; and / or

  (b) it is not possible to use the GCSx secure email method.

- Users should refer to the "Encrypt and Send Email Guide for Internal Users" and the "Encrypt & Send Secure Message Centre Email Guide (for external users)".

N.B. Where the GCSx secure connection is available this must be used instead of Encrypt and Send.

4.5. Transfer of electronic data via the internet using File Transfer Protocol (FTP & Secure FTP)

The File Transfer Protocol (FTP) is a standard network tool used to transfer computer files from one host to another over a TCP-based network, such as the Internet. This is not normally available to users without contacting IT.

- Standard FTP without encryption is inherently insecure and must not be used for transmitting any controlled data under any circumstances.

- Secure FTP (SFTP) file transfers are acceptable for transferring controlled data. This should be arranged via Barnet IS department. Secure FTP (SFTP) uses the Secure Shell protocol (SSH) to transfer files. Unlike FTP, SFTP encrypts both commands and data, preventing passwords and sensitive information from being transmitted openly over the network.

It is the responsibility of the sender to ensure that the use of such a system is appropriate for the use they propose. If in doubt, seek advice from the IS Security Manager, email dennis.hunt@barnet.gov.uk.

(C) Copyright London Borough Barnet 2016

4.6. Removable storage devices (CD, DVD, USB drive & memory stick)

When the size of the data being transferred or other restrictions (such as non-availability of FTP or SFTP) make email transfer methods inappropriate, removable media should be considered to transfer data.

Where you are considering the transfer of controlled data the media used to perform encryption must conform to the AES 256 standard.

Where a user has a machine with CheckPoint End point Security installed, an **enabled USB port** and an approved encrypted USB memory stick the user may be able to perform the operation of writing the data themselves. An enabled USB port will only be available to users who have been granted a policy exception (see Policy Exceptions Policy). The information transferred to the approved encrypted USB memory stick will be automatically encrypted. However the provisions required for communication of passwords detailed below must still be followed.

For users who are required to write (copy / move) data to removable media and the **USB port is not enabled** on your computer or the quantity of data to be transferred is too large for memory stick, or CD/DVD, then assistance should be sought from IS.

- Where a removable/portable storage device is used, copying will be undertaken by IS to an encrypted data stick.
- All removable or portable storage devices used for data transfer must be encrypted by IS to AES 256 standards.
- Ownership of the media used must be established. The media must be returned to the owner on completion of the transfer and the transferred data must be securely erased from the storage device after use.
- Encrypted portable storage devices must be password protected with a strong password as set out in the council's Password Policy. The password itself must be conveyed to the third party in a separate communication from that covering the controlled data itself.
- You should provide clear instructions on the recipient's responsibilities and instructions on what to do if they are not the intended recipient.
- An accompanying message or filename must not reveal the contents of the encrypted file.
- The sender must check at an appropriate time that the transfer has been successful and obtain a receipt. An email confirming receipt is acceptable. Report any issues to their line manager and in the case of missing or corrupt data to IS and IMT immediately.

(C) Copyright London Borough Barnet 2016

4.7. Telephone / mobile phone

As phone calls may be monitored, overheard or intercepted either deliberately or accidentally, care must be taken as follows:-

- Controlled data must not be transferred / discussed over the telephone unless you have confirmed the identity and authorisation of the recipient.
- When using answer phones do not leave sensitive or confidential messages, or include any personal data. Only provide a means of contact and wait for the recipient to speak to you personally.
- When listening to answer phone messages left for yourself, ensure you do not play them in open plan areas which risks others overhearing.

4.8. Internet based collaborative sites

The use of peer to peer (P2P) or 'cloud' file sharing programs such as 'Dropbox', Google Docs or Office 365 to exchange controlled data over the internet is not permitted unless specifically authorised by the IS Security Manager. They are inherently insecure if not implemented in a secured corporate environment.

Where you believe you have a requirement to use this type of transfer you must speak with the IS Security Manager who will provide appropriate advice.

Some organisations have secure portals for the transfer of information using appropriate protocols (SFTP etc.). These may be used after confirming that the organisation is entitled to receive the information and the portal is secure.

If in doubt you should check with the IS Security Manager

4.9. Sending information by post

As a local authority we will routinely send letters containing personal information to our customers for example in connection with council tax or benefit claims. However, whilst this is routine, care must still be taken to ensure that the information is correctly addressed to a named recipient and information is not sent in error to the wrong recipient. Mail going to the wrong person is a danger to the individual whose information is being sent. It also puts the council at risk of breaching our responsibilities under the DPA.

You, as the sender, are responsible for making sure that:

- The postal address is correct.
- The envelope is clearly marked for the attention of the intended recipient.
- No information relating to another customer / service user has been included in error, either in a letter/email or an attached document.
- That you choose the most appropriate method of transfer.

(C) Copyright London Borough Barnet 2016

You are responsible for the package up until its successful arrival at its destination. You must therefore ensure you choose the most appropriate method of transfer and mitigate any potential loss or risk to the information.

Posting of sensitive / confidential data

An extra level of protection must be applied when sending:

- a large amount (e.g. a file) of personal data (as defined by the DPA)

  or;

- Any amount of controlled data.

It is essential that the document or file, whether sent on a media device or in paper form, is kept secure in transit, tracked during transit, and delivered to the correct individual. So you must ensure that:

- the package is securely and appropriately packed, clearly addressed and has a seal, which must be broken to open the package.
- the package must have a return address and contact details.
- the package must be received and signed for by the addressee, e.g. the use of special or recorded delivery.

Successful delivery / transfer of the item must be checked as soon as possible. Any issues must be reported immediately to your line manager.

NOTE:

Staff members or teams who wish to send sensitive information in a way different to that prescribed above, must apply for a formal policy exception as outlined in the council's Policy Exception Policy, stating clear business reasons as to why an exception is required. An exception should be sought for one off requests as well as requests for an alternate way of working. Any exception granted will be reviewed annually.

Staff and managers who do not abide by the above requirements will be in breach of council policy, which may lead to disciplinary action.

4.10. Use of internal mail

The electronic sharing of information is preferable. However, where the use of internal mail is deemed appropriate, you must ensure that:

- post sent through the internal mail system is clearly and correctly addressed to the intended recipient.
- files or documents containing controlled data must not be transferred loose and should be appropriately packaged, in a sealed envelope, to avoid disclosure to others or loss of information.

(C) Copyright London Borough Barnet 2016

- if information is deemed reasonably high risk if lost or mislaid, where possible this should be hand delivered to the recipient department.

4.11. Hand delivery / collection

Hand delivery or collection of a document is also an approved method of transfer. Remember however, if you are taking paper records off site you still need to ensure you are complying with the Paper Records – Secure Handling and Transit Policy.

Also when arranging for an individual to collect information, you should satisfy yourself that they are who they say they are and seek an appropriate form of identification before you hand over any documentation.

5. Transferring data outside of the United Kingdom / EEA

You must speak to the Information Management Team before agreeing or undertaking any transfers of any data outside of the EEA. This is especially important when handling controlled data.

You must check, as part of information management due diligence that any service providers you procure are not planning to process personal data outside the EEA. E.g. some service providers may use cloud based systems for data storage which are not UK based.

Principle Eight of the Data Protection Act 1998 (DPA), requires that personal data must not be transferred to a country or territory outside the European Economic Area (EEA) unless the country or territory can provide an adequate level of protection for the rights and freedoms of the individuals whose data is being transferred.

It is important to note that all other principles of the Data Protection Act are still relevant and must be complied with.

6. Reporting data incidents

Staff must report any suspected or actual security breaches related to data transfer in line with the council's Security and Data Protection Incident Management Policy available on the intranet.

7. Policy review

This policy will be reviewed on an annual basis or sooner as is required where there are changes in legislation or recommended changes to improve best practice.

(C) Copyright London Borough Barnet 2016

8. Associated policies

This policy forms part of a suite of Information Management policies which are all available on the intranet. The policies provide further guidance on council information standards, data security and working practices which must be adhered to.

Further advice and guidance on transfer methods is available from the service desk

Email: ITService.desk@barnet.gov.uk

Tel: (020) 8359 3333 or dial ext: 3333

If you are in any doubt whether a transfer can be undertaken in line with the Data Protection Act, please seek advice from the Information Management Team.

Email: data.protection@barnet.gov.uk

Tel: (020) 8359 2029 or dial ext: 2029

(C) Copyright London Borough Barnet 2016