# Data Security and Encryption Policy

## Version Control Sheet

| | |
|---|---|
| ***Title:*** | Data Security and Encryption Policy |
| ***Purpose:*** | To advise staff of the Council's policy and procedures regarding data security and encryption |
| ***Owner:*** | Data Protection Advisor<br>lhenley@thurrock.gov.uk<br>01375 652500 |
| ***Approved by:*** | |
| ***Date:*** | March 2019 |
| ***Version Number:*** | 1.0 |
| ***Status:*** | Draft |
| ***Review Frequency:*** | As and when changes take place to Information Governance Legislation. |
| ***Next review date:*** | As above |

**Amendment History / Change Record**

| Date | Version | Key Changes / Sections Amended | Amended By |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

## CONTENTS

## 1. Introduction

Information/data security is vital to Brentwood Borough Council in the delivery of services to residents, businesses and visitors. The availability, integrity, security and confidentiality of information held is essential to ensure compliance with Data Protection legislation.

It is important that citizens are able to trust the Council to hold personal information securely when obtaining and holding information. This policy is designed to provide an appropriate level of protection to the information and data for which the Council is responsible for.

## 2. Background

The Council is required to comply with the principles of Data Protection legislation. They are sometimes referred to as the "principles of good information handling". They apply to all personal information including the fundamental principle that covers the security of personal information.

Following the recent highly publicised losses of personal data by various Government agencies, the Council has implemented encryption and secure data transfer software as well as permissions-based access across the Office 365 suite as an enabler to ensure that Council's data can be secured during electronic transfer and to prevent such data being intercepted.

The Council has gone to great lengths to ensure that the methods offered to partner organisations for the sharing of data are as secure and flexible as possible.

## 3. Scope

The scope of this policy is:

- To ensure that staff are made aware of the encryption and secure transfer processes that are now in place within the Council.
- To ensure that staff are made aware of the importance and need to hold personal information securely (both electronic and manual records).
- To ensure staff are fully aware of their responsibilities when storing data on portable media devices such as laptops and memory sticks.

## 4. Encryption and Secure Data Transfer

All staff should be aware of and comply with the following:

- All Council data must be stored on approved council systems.
- Internal and External emails containing **OFFICIAL** information can be sent via normal email (irrespective of who these are sent to e.g., police, resident).
- **OFFICIAL-SENSITIVE** emails that are sent internally must be classified as such and can be sent via normal email.

- **OFFICIAL-SENSITIVE** emails that are sent externally must be classified as such and sent via:
    - Your standard email address if the recipient is a public sector body (e.g. council, police, NHS etc.).
    - CitrixFileShare if the recipient is not a public sector body (e.g. resident, supplier).
- *If you need to send personal data within or outside of the Council then contact Data Protection team or the ICT about secure delivery mechanisms* **-** . Personal data should only be sent when absolutely necessary, and must be delivered securely. In some cases, information can be anonymised to prevent identification of individuals (e.g. remove names and address and use a shared code reference instead that is known by the recipient). The Data Protection Team can provide advice on how this can be best achieved.
- The Data Protection Team can provide advice on whether any data you have would be regarded as personal data. This team can also provide advice on encrypting files and how to securely transport files to contractors and partners.

## 5. Security of data held on portable devices (such as laptops, Chromebooks, mobile phones and memory/USB sticks)

The use of portable devices are subject to extra requirements because of the increased security risk these devices pose to information held by the Council.

All staff should be aware of and comply with the following guidelines:

- Do not store Council data on unencrypted transportable media **-** Transportable media is basically anything that can easily be removed from the office, so things like USB memory sticks, CDs, DVDs, floppy disks, etc Should not contain unencrypted data. Do not store Council data on an unencrypted laptop. If you use a Council laptop you must ensure the laptop is encrypted. Only use USB memory sticks provided by ICT as these are appropriately encrypted.
- If a portable device is shared amongst several users then a procedure (e.g. a log showing where the device is) must be in place to record the whereabouts of the device at all times.
- Security of the device is the responsibility of the user at all times.
- Lock the device away in a secure place when it is not in use.
- Be aware of the additional security risks if leaving your device unattended or travelling with your device. Lock your device if not in use.
- Do not install any software on the device – this must only be carried out through the ICT Helpdesk.
- Exercise caution when connecting the device to any foreign networks e.g. Home PCs, Bluetooth, Wireless etc. and do not transfer and store Council data on foreign networks.
- Personal record keeping, correspondence or games on a mobile device should be limited and undertaken in personal time.

- Incidents involving the loss or theft of a mobile device owned by the Council should be reported immediately to the Data Protection team or theICT Manager.

## 6. General Data Security

All staff should be aware of and comply with the following guidelines:

- Do not save and/or store Council data on non-Council equipment. This includes a private PC, private laptop, private mobile device, internet café PC's, personal transportable media etc. Council procured encrypted memory sticks should be used for this. Those staff who cannot comply with this should contact ICT/ the Data Protection Team for advice.
- Never give your password to anybody **-** If you believe somebody else knows your password, please change it immediately and inform ICT/the Data Protection Team if you think there may be a problem.
- If you move personal records away from your base location, then these records must be held securely at all times.
- If you currently have personal data, which is stored insecurely, you must secure it immediately - You must remove any personal data from insecure locations.
- If you become aware of any loss of Council data you must contact the Data Protection Team immediately **-** The loss of any personal data is a serious matter and must be reported without delay, providing as much detail as possible.
- If you become aware of any personal data that is not stored securely report this to the Data Protection Team immediately - This could be manual records stored in filing cabinets that are not locked.

## 7. Standards for Secure Document Management

As an employee, elected member, agency worker, third party organisation or other authorised personnel, it is your responsibility to maintain the security of information owned or held by Brentwood Borough Council by ensuring that it is accessible to those authorised to access it, and that it is not accessible to anyone else. An important aspect of this security is achieved through the storage of information. These standards apply equally to manual records, electronic records and emails.

All staff should be aware of and comply with the following guidelines:

- All records (manual and electronic) must be held securely. Records and ICT equipment (that contain records/data) must not be left in insecure locations (e.g. left in vehicles).
- You should store documents to allow access to authorised users and appropriately restrict unauthorised users. This can be achieved through information technology (ICT) security controls on network folders, documents and files or physical measures on rooms, cupboards or cabinets.

- You should not store confidential and non-confidential documents under the same access control.
- You should regularly review (at least annually) stored documents, files and folders in line with the Council's document retention policy.
- When disposing of documents, files or folders, then this must be undertaken securely.
- If you are responsible for shared documents, you should ensure that you understand your responsibilities and have the skills necessary to control access appropriately.
- If you are a Manager, then it is your responsibility to ensure that all documents created or stored within your service area are appropriately managed in line with the principles of Data Protection legislation.

## 8. Key Points to note:

- The Authority's data and information is valuable and must be protected at all times.
- Users should be conversant with and comply with this policy and all ICT/Information Security policies including supporting policies/practice guides.
- Suspected breaches of the policy must be brought to the attention of a line manager, Data Protection Team or the ICT Manager immediately.
- Breach of the Information Security Policy or failure to report a breach could result in disciplinary action.