THE Fallibroome TRUST

Data Encryption Policy

All Trust Staff

DISTRIBUTION	This is a Trust-wide policy and applies to all staff within the Trust.		
DOCUMENT ID	FT-IT007 Data Encryption Policy		
AUTHOR	HRS	**VERSION**	1.1
RATIFIED BY THE DIRECTORS OF THE FALLIBROOME TRUST			
POLICY REVIEW CYCLE		3 YEARS	
POLICY REQUIREMENT		NON-STATUTORY	

CONTENTS

INTRODUCTION

The Fallibroome Trust takes its responsibility for obtaining, using and storing data seriously. As such, it wishes to ensure that all data held by the Trust electronically is adequately protected from loss and inappropriate access, whether by accident or theft. Furthermore, under the Data Protection Act (the UK's implementation of the General Data Protection Regulation GDPR), the Fallibroome Trust is required to have in place appropriate policies and procedures which ensure the secure storage of data covered by these regulations at all times.

PURPOSE

To reduce the risk of unauthorised access to data held by the school on electronic and mobile devices The Fallibroome Trust has established a comprehensive policy of data encryption. This covers data which can be accessed from outside the school and which can be removed from the school.

This policy covers data stored by the following means:

- Laptops
- Handheld portable devices such as mobile phones, PDAs and Tablet devices
- Portable storage devices such as USB data sticks, external drives
- Removable media such as DVDs, CDs etc…

GOVERNANCE

The Local Governing Body is a committee of the Fallibroome Trust. The Local Governing Body will adopt and comply with all policies communicated by the Directors of the Trust. The Local Governing Body is responsible for setting out the policies and practices for staff. The Local Governing Body may delegate these matters to:

- The Principal/Head teacher;
- A sub-committee of the Local Governing Body; or
- A sub-committee and the Principal/Head teacher.

Where this procedure refers to the Local Governing Body representative this can be any one of the above.

SCOPE

This procedure applies to all employees of the Fallibroome Trust. It is supported by several other Fallibroome Trust or Local School policies or guidelines, notably:

- FT-IT001 - Acceptable Use Policy (Staff)
- FT-IT004 - eSafety Policy
- FT-IT005 - Data Protection - Main Policy
- FT-IT014 - Email Policy - Staff

IMPLEMENTATION

Encryption will be applied to relevant devices located on all Trust premises, in order that data stored on them will be automatically encrypted. Staff using these devices will not be asked to supply a specific password for individual documents or files (unless there is a specific need for a document to be password protected/encrypted) once they have logged into their device.

Handheld portable devices such as mobile phones and tablets will be required to meet the Trust's encryption policy before connecting to Trust secure data systems. If a handheld device cannot be encrypted it must not be used to store **person identifiable data** (see below). Furthermore, it must not be connected to any other of the Trust's secure systems, whether by physical (e.g. USB) or wireless connection (e.g. Wi-Fi). If there is a BYOD (bring your own device) or Guest Wi-Fi network available then connection to these networks will be permitted.

The Fallibroome Trust **PROHIBITS** the use of non-encrypted data storage for GDPR (General Data Protection Regulations) assigned "Personal" or "Special" data categories on portable storage devices, such as USB data drives. These categories are defined as:

- **Personal data**
  The GDPR applies to "personal data" meaning any information relating to an identifiable person who can be identified (directly or indirectly) in particular by reference to an identifier.

  This definition provides for a wide range of personal identifiers to constitute personal data, including for example (in the Trusts case, but not limited to) pupil name, student ID, staff ID, location data, date of birth, pay grade, pay details, overtime pay, NI Number, sex etc..

  Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

- **Sensitive personal data**
  The GDPR refers to sensitive personal data as "special categories of personal data". The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

If storage of this information is required, a Trust approved FIPS 140-2 Level 3 certified USB device is required. Only Fallibroome Trust purchased USB drives (Kingston Iron Key D300 - managed) may be used.

Removable media such as CDs and DVDs will also be encrypted, if appropriate.

If you copy data from an encrypted Trust USB or other device to storage on your personal home computer or laptop this data **MUST** be encrypted if retained, or, securely deleted immediately after use. It is staff member's personal responsibility to ensure that this procedure on home use is complied with; it is not the responsibility of the Fallibroome Trust to supply software or services for a personal device.

COMPLIANCE

- The school’s encryption policy recommends the use of devices that support the FIPS 140-2 standard

- Passwords will be kept confidential by staff and will adhere to the guidelines defined in the school's eSafety policy

- Staff will not remove or copy sensitive or personal data from any Trust premises unless the data storage device is encrypted and is transported securely for storage in a secure location

- Staff are reminded that Emails should be treated as public property and therefore should contain as little personal data as is possible

- Staff must protect all portable and mobile devices used to store and transmit personal information using approved encryption software

- Sensitive or personal data must be securely deleted when it is no longer required

- Non-compliant devices may be detected and disabled using management systems installed for this purpose without notice

- Staff will not publish any documents containing personal data on externally accessible websites

- Staff must securely delete sensitive or personal information from their systems once it is no longer required

- Regular monitoring checks will be undertaken to ensure compliance with the criteria set out above

- All incidents resulting in a breach of these guidelines must be reported to the Trusts IT Department (suppport@fallibroometrust.com) and the Trusts Data Protection Officer immediately

- According to ICO regulations, the Trusts Data Protection Officer will inform the ICO if there are any losses of personal data