Encryption Policy

For the attention of:	All Staff
Produced by:	Group Executive Director of Technology
Approved by:	SLT
Date of publication:	June 2025
Date of next review:	January 2026

WINDSOR FOREST COLLEGES GROUP

Vision, Purpose & Values

Our Vision

Our students will be recognised locally & nationally for their positive impact on the communities and industries in which they choose to work.

Our Purpose

To inspire our students to gain the skills, knowledge and behaviours they need to be resilient and thrive in an ever-changing world.

Our Values

Excellence: A culture of creativity, high expectations, ambition and aspiration

Respect: Showing fairness, courtesy and mutual respect to each other and our environment

Integrity: Honesty, openness and trust at the heart of College life

Diversity: Celebrating diversity and inclusivity as a key to our success

Contents

1. Introduction

The Windsor Forest Colleges Group (the College) has a duty both under law and for its own business purposes to ensure that college data, especially data covered by the Data Protection Act and UK GDPR is stored in a secure manner, and that only authorised users can gain access to it. There are a number of different controls that the college can put in place to achieve this end, and the college must determine the most appropriate set of controls to deploy for each different situation. One of the controls available to the college is data encryption. This policy sets out the situations in which encryption will be used as an appropriate control measure.

This policy is non-contractual and may be altered by the College at any time.

2. Data at Rest Encryption

In the context of data handling systems, "data at rest" refers to data that is being stored in stable destination systems. Data at rest is frequently defined as data that is not in use or is not traveling to system endpoints, such as mobile devices or workstations. This includes servers, pcs, laptops and any other electronic device used to access College Data.

3. Desktop Computers

Standard desktop computers are classified as a low level of risk. These devices are not used to store data defined under UK GDPR (ie data about identifiable indivduals, referred to as personal data) and are unlikely to be stolen and as such do not generally require to be encrypted.

Where there is high use of personal data these devices will be protected by whole device encryption. These are devices that have a high level of access to systems such as HR, Finance and the MIS system.

Staff must always ensure to save to the network drives / approved cloud storage and not use the local device to store any files.

4. Laptops / Tablets / Mobile Phones and Other Mobile Devices

The College will ensure that all portable college provided staff devices will be protected by appropriate whole device encryption.

Student portable devices are classified as a low level of risk and as such will not be encrypted.

Staff must always ensure to save to the network drives / approved cloud storage and not use the local device to store any files. The only exception to this is to use the Microsoft Offline files feature when they are away from college which is enabled by default.

A VPN is also provided to allow staff to securely dial in from home to access (not not download) files on central servers.

Where staff choose to have college email enabled and stored (this does not include using webmail) on their personal devices such as Android and Apple they are required to ensure that the device is protected by two-factor authentication to ensure that device encryption is enabled.

If a staff member is unsure whether or not their device is encrypted, they must either not have email on their device or seek guidance from the IT Services Team.

5. Removeable Media (e.g. Memory Sticks, USB Keys, External Hard Disks)

The College would strongly prefer that all confidential information and personal data is kept on the College's networks/approved M365 / Google cloud storage and not copied to removable media. However, it recognizes that on occasion (such as [insert examples] it may be necessary to transport confidential information or personal data on such media

Any confidential information or personal data which needs to be transported on removeable media must be stored on a hardware encrypted memory stick / usb key, which is provided free from the IT Services Team.

Staff must not use any other removable media device to store such data..

6. Cloud Based Storage

The storage of confidential information and personal data on cloud based systems are restricted to the Google Suite (for teaching purposes) and Office 365 Systems (for all purposes). No other cloud based systems should be used for the storage of this type of data. The only exception is when transferring data to approved Exam systems for students to complete their qualification.

7. Data Transmission Encryption

Any confidential information or personal data transferred off the College systems to another system must do so using encryption.The IT Services Department can analyse these systems and offer advice to users on how to achieve this

All College systems configured by the IT Services Team that are available onsite and offsite have appropriate encryption enabled to ensure that the data transmitted cannot be intercepted.

No system should be set up without approval from the IT Service Team.

8. Email

Any confidential information or personal data that is transmitted via email (whether in the text of the email or as an attachment) to an external domain (i.e.. not a college email address) must be sent as an encrypted email or using secure share links from approved Cloud Storage.

This can be using Egress which can be installed by the IT Services Team or by putting the word Encrypt or Encrypted in the Subject line of an email. The system will then automatically encrypt the email and send an email with a link to the recipient who then must prove who they are in order to see the message.

9. Associated Documents

- UK GDPR Policy