'Christ at the centre, children at the heart'

Our Lady of Walsingham Catholic MAT
Company No: 08444133
Registered Office: Fordham Road, Newmarket, Suffolk, CB8 7AA

Approved by the Trust Board:	**March 2026**
Signed by Trust CEO:	
Review Date:	**March 2029**

Addition to the OLOW Acceptable Use of IT Policy: Introduction of MultiFactor Authentication (MFA)

1. Introduction

In accordance with the Department for Education (DfE) Digital and Technology Standards, the Trust will be introducing **MultiFactor Authentication (MFA)** across all appropriate systems. The DfE identifies **robust cyber security controls**, including **MFA**, as a core expectation for schools and trusts to ensure safe and secure access to digital systems.**-Factor Authentication (MFA)**

2. What is MultiFactor Authentication (MFA)?

MFA is a security measure that requires users to verify their identity using **two or more independent factors** before accessing Trust systems. Typically, these factors include:

- Something you *know* (e.g., your password)
- Something you *have* (e.g., an authentication app or hardware token)
- Something you *are* (e.g., biometrics, where applicable)

3. How MFA Works

When logging into a Trust system, users will:

1. Enter their usual username and password.
2. Receive a prompt to confirm their identity via a second method—most commonly:
    - An authentication app on a mobile device
    - A generated code
    - A hardware device (dongle)

This additional layer of security significantly reduces the risk of unauthorised access and strengthens the Trust's cyber security posture in line with DfE standards.

4. Why MFA Is Needed

The Trust holds sensitive data, including personal, financial, and safeguarding information. The DfE identifies cyber security as a core standard and specifically expects:

- Strong identity governance
- Secure authentication measures
- MFA across all appropriate systems

MFA helps protect against:

- Compromised or stolen passwords
- Phishing attacks
- Unauthorised access to Trust systems and cloud services

Implementing MFA is therefore essential to meeting compliance expectations and ensuring the safety and security of Trust data.

5. Use of Personal Devices for MFA

For convenience, staff **may use their personal mobile device** to receive or generate MFA authentication codes using a Trust approved authentication app (Microsoft Authenticator -available from the app stores). This method is secure, easy to use, and recommended for most users.-approved authentication app

No personal data from the device is accessed by the Trust or by the authentication application.

6. Provision of Hardware Dongles

Staff who are **not comfortable using a personal device** for MFA may request a **Trust issued authentication dongle**.-**issued authentication dongle**

- The dongle will be issued by the Trust at no cost to the staff member.
- Staff must **sign for the device** on receipt.
- The dongle remains Trust property and **must be returned at the end of employment** or when otherwise requested.

7. Staff Responsibilities

All staff are required to:

- Comply with MFA requirements
- Keep authentication devices secure
- Report lost or stolen devices immediately
- Use MFA only in the Trust approved manner approved manner