

Remote Access Policy

For Schools



Introduction

The purpose of this policy is to allow greater flexibility to school teachers/staff by allowing them to access school resources remotely.

The Remote Access system provided via Flintshire's Traded Service is called DUO, a secure, encrypted connection, this is the only permitted method of remotely accessing schools' IT Systems.

For all its benefits it should be realised that remote access does not come without risks and as with any other IT related service, the Traded Service needs to ensure that the use of remote access is organised and controlled in a manner which will be beneficial to the safety, integrity and reputation of Flintshire County Council and ensure that its use contributes to the delivery of efficient services.

This policy is to be read and followed in conjunction with your school's other policies and procedures including your Teachers/Staff Code of Conduct, GDPR policy and Social Media Policy.

Scope

The remote access facility provided to teachers/staff members who have been permitted access include, but are not limited to:

- SIMS
- P2P
- Masterpiece
- Workspace
- InTouch
- SchoolComms
- TOPdesk
- A2C

Any facilities which are withdrawn or retired by a provider may be automatically removed from the remote access system.

Aims of the Policy

1. To ensure as far as possible that both managed and personally owned devices used by teachers/staff for work purposes are operated in a manner which protect confidentiality and school data.
2. To ensure the appropriate and secure use of remote access and its applications.
3. To ensure the appropriate and secure use of remote access facilities are available to teachers/staff is clear.

Remote Access Policy

For Schools



4. That all school data is kept in accordance with GDPR and schools data retention policies.
5. To ensure devices meet the prerequisites of the remote access systems, these include up to date operating systems, latest updates and antivirus.

Definition of Terms

This policy makes references to several terms throughout and clarity on the meaning is below

- Managed device - a school device, PC or laptop provided by school
- Unmanaged device – a personal device, PC or laptop from home
- Operating Systems - Also known as an 'OS' – This is the low-level software that supports a devices' basic functions
- ICO – Information Commissioners Office
- Traded Service - purchased by schools using a delegated ICT budget as part of the Education ICT Service Delivery provision
- SIMS – Schools Information Management System
- P2P – Purchase to Pay
- Masterpiece – (FMS) Financial Management Solution
- Workspace – for reporting staff absence, school closures, accidents
- InTouch – Sending of messages between school any person recorded in your SIMS system
- SchoolComms – payments for school trips, dinner money payments
- TOPdesk - Service management software for logging helpdesk jobs
- A2C – data exchange between different examination boards

Use of Personal Devices and Support

Due to the pace of change in technology and the need to maintain robust security standards, it is not possible to support all models, manufacturers and operating systems and the current support situation will continue to be reviewed as technology and cyber security threats evolve.

Remote Access Policy

For Schools



Security and Data Protection

By enrolling in the Traded Service's remote access solution, employees must accept that the Traded Service will enforce security controls, which will include, but are not limited to, the following:

- General access to applications is secured through the use of a password which must be set by the teacher/staff member upon enrolment of their managed/unmanaged device with the service. This password must meet the complexity requirements stated by the application.
- Security certificates issued by the Traded Service shall be installed on managed/unmanaged devices to allow for management of applications and data.
- Teachers/staff are expected to keep the operating system of their unmanaged device at the latest version available to it and that antivirus and Windows updates are updated as newer versions are published.
- Schools as the data controllers are accountable for GDPR compliance and could face disciplinary action in the event of a data breach. All data breaches that could harm the rights and freedoms of individuals must be reported to the ICO.

Third Party Remote Access

Third party suppliers requiring access to school data will be provided by the Traded Services' remote access solution.

Costs

Access to schools' remote access service is subject to a software licence fee charged per user annually to school. Any decision to terminate a licence must be notified 5 days prior to termination to the Traded Service via TOPdesk.

Monitoring

Monitoring and reporting on licencing is undertaken on the remote access service.

Advice and Guidance

Advice and guidance on remote access is available from the IT Business Partner for School

