



**St John's
School**
Achieving Together

Article 28: You have the right to a good quality education.

Article 23: You have the right to special education and care if you have a disability, as well as all the rights in this Convention, so that you can live a full life.

Remote Working Policy

Policy Status: Recommended

Review Cycle: Annually

Owner: Designated Safeguarding Lead

Date: February 2025

Approved by: SLT

Date: March 2025

Review Date: March 2026

Introduction

The underlying principles of this guidance are:

- Individuals are responsible for the data they are authorised to handle outside of the organisation and reasonable steps should be taken to secure data taking into account its value, sensitivity and confidentiality.
- St. John's School are responsible for the preparation of appropriate services to enable work out of school and to support staff in its execution.

Work Out of School Definition and Purpose

In this guidance statement, home working is defined as a formal arrangement where the member of staff is permitted to take work home overnight, at weekends, over the school holidays or in emergency situations to complete projects or ad hoc work. This guidance provides direction on how to safeguard electronic and physical data, including personal and non-personal data. It also covers the circumstances where data is taken out of school for work purposes, for example, to make home visits by attendance officers or by SLT for external meetings.

It covers all information handled on behalf of the organisation including data that is:

- accessed
- collected
- used
- shared
- stored
- disclosed
- disposed of

Expectations

All HR procedures will continue to be followed, so if a Leave of Absence is required for an appointment, staff members are sick and unfit for work or unable to work for any reason then they should call into the absence line as normal. Leave of Absence requests can be forwarded to the HR mailbox at sjs.hr@biltt.org. If any employee does not follow this guidance they could be subject to disciplinary procedures or subject to a review of their salary. Any correspondence regarding HR matters should be directed to sjs.hr@biltt.org. Confidential HR matters can be directed to the Headteacher.

Criteria for Taking Data Off-Site

Where data is taken off-site each member of staff should have approval from management, who will have considered the following;

- The type and volume of data that can be moved off-site. This must be limited to only that which is required to complete the processing activity
- The purpose for which it is being taken
- The methods for transporting data off-site (physical and electronic)

Staff working from home must first have agreement from their line manager to take and store work at home.

- The amount of home working expected, with maximum time limits

- The type of work that can be completed at home
- A safe environment for working at home
- Any requirements for reporting on home working

Work taken off-site must not be worked on in a public location and public wifi should be avoided. Prior to any agreement, St. John's School will ensure that the data and processing out-of-school is documented and risk assessed by the Data Protection Officer.

Communications with pupils must only ever take place using approved organisation communication protocols (e.g. using organisational email, not personal email accounts; using approved systems such as Google Classroom or other virtual learning environments).

Organisational communication, email and acceptable use policies must be followed when conducting work, even on a personal device.

Transportation of Data

The greatest risk of data loss is when it is being moved.

Where possible access files using a secure, access-controlled cloud environment and avoid physical transportation of documents and storage devices.

- Physical files (paper documents) must be kept secure and in possession of the user at all times. No files will be left unattended in a vehicle or other unsecured location during transit.
- Use of USB memory sticks (or other portable storage) is not allowed.

In all cases follow these steps:

- Management should agree the scope of off-site working (see criteria for taking data off-site) and the methods of offline working
- Where access to data is not through cloud storage, remote desktop or virtual private networks, save any data on to an encrypted device whilst on-premise.
- Where any physical data is being moved, record its removal from the site and ensure a signature of the custodian is obtained.
- Physical files (paper documents) must be kept secure and in possession of the user at all times. No files will be left unattended in a vehicle or other unsecured location during transit. Where possible, reduce the visibility of documents in transit and when being stored.
- Physical devices (laptops/portable storage) must meet the standards set in the IT Policy. At a minimum, any devices must be encrypted.
- When working at the remote site, ensure that access to data is safeguarded. Do not share access to documents with non-authorised personnel and do not share the use of any device with not-authorised personnel. Do not share any passwords. Minimise screens if others can view data. Lock or turn off devices when not in use.
- Physical confidential files must be kept securely (e.g. store in a cupboard, drawer or briefcase)
- When back on premises, return all data and physical devices to their secure locations and the custodian should sign for the return.

Health & Safety

It is the responsibility of the employee to care for their own Health and Safety including taking regular breaks and make the school aware of any issues that may have an impact on this. Accidents to employees sustained while working at home must be reported in the same way as if office based.

Home Office Arrangements

Staff working at home will ensure the confidentiality and security of any information they are required to work within the home, in accordance with their existing contract of employment, the organisational IT Policy, Data Protection Policy and Staff Code of Conduct.

Such information will not be accessible to family or visitors of the home worker and must be securely stored at all times whilst not working on the document.

Working in Public

- Working on private, confidential and personal data in public areas should be avoided.
- Working via public WIFI should only take place if you have a VPN.
- Use of public computers is not allowed.

Using Your Own IT Equipment

At a minimum, if using your own equipment it must meet minimum standards for anti-virus, malware and operating system updates and security patches.

Personal devices accessing organisational data should employ access control to prevent access by unauthorised users. Consider setting up a work-specific profile. Use multi-factor authentication and secure passwords.

Avoid downloading documents to your home IT equipment. Where possible, share information via SharePoint, especially for staff resources. If you have no choice but to download a document to work on, discuss with your school leadership team prior and once you have completed and uploaded the document, delete from your home device and empty the recycle bin as well.

If you must download documents to your own device, create an encrypted folder and remove this folder from any synchronisation with personal backup solutions.

Remember, documents can be saved in SharePoint or emailed to your work address to ensure no documents have been stored in your personal cloud space or backup.

Cloud Access to Services (e.g. Google drive, Office 365, Cloud MIS, CPOMS etc)

You should avoid downloading to your own device and work on the document online.

Using Portable Storage

USB sticks/portable hard drives and other portable storage should be used for short-term transportation of data only and only in exceptional circumstances. All files should be stored on the organisation's network and only required files stored on the device and then returned onto the network at the earliest opportunity and files on the device deleted. Any use of portable storage must be approved by management and only when encryption is available on the device.

Any devices or equipment provided by the employer for home working should be returned when the home working arrangement ends.

Insurance and Related Matters

The employer will extend its employer, public liability and professional liability insurance to cover staff working from home and taking data off-site, ensuring coverage of assets and data during transportation as well as storage at home. The organisation will ensure that any organisational equipment has adequate insurance cover for the locations it is used and during transportation.

Availability of Data

Whilst data may not be physically held by the organisation, the organisation must be able to retrieve and make available any such data in response to subject access requests under the Data Protection Act 2018, or Freedom of Information requests under the Freedom of Information Act 2000

Data Breaches and Information Incidents

If a data breach or information incident contact school management and the Data Protection Officer immediately, following the organisation's Data Breach Procedure. This would include (but not be limited to) unauthorised disclosure or loss of equipment.

Data Protection Education can be emailed at dpo@dataprotection.education, or a data breach can be logged on the Data Protection Education Knowledge Bank.

Absence and Sickness

If an employee is unable to work on the day which they had expected to work from home due to sickness, injury or otherwise, they must follow St John's School absence reporting procedure. The employee is required to keep the Headteacher informed of the likely date of return to work, the reason for the absence, and progress, as if they were normally attending work.

Disciplinary Procedures

The "Employee Disciplinary Procedure and Code of Conduct Policy" apply equally to office-based and working from home arrangements. Any abuse of the working from home arrangements amounting to misconduct may be subject to disciplinary action.

Confidentiality

While working from home employees will remain subject to all confidentiality clauses contained within their contract of employment. A disclosure of confidential information during the course of employment may be considered by the school as gross misconduct and grounds for termination of employment without notice.

Monitoring and Review

The line manager will be responsible for monitoring the employee's performance while working occasionally from home.