PolyMAT

Remote Working Data Protection Policy

Reviewed: November 2023

Approved: December 2023

Revision due: December 2024

Remote Working Data Protection Policy

Scope and Definitions

This policy applies to all staff whilst working from home and/or are using or accessing Trust systems or information while working remotely. This includes individuals who are given access to the Trust networks and Trust data (including governors, students, visitors, volunteers, contractors and third parties). It applies to information in all formats, including paper records and electronic data.

Remote working means working away from the Trust or school sites. This includes working while connected to the Trust's networks.

A mobile device is defined as a portable device which can be used to store or process information. Examples include but are not limited to laptops, tablets, USB sticks, removable disc drives and smartphones.

Awareness of Risk

Working remotely presents both significant risks and benefits.

Staff may have remote access to information held on secure Trust servers but without the physical protections available in a school. Without the network protections provided by firewalls and access controls, there are much greater risks of unauthorised access to data as well as a risk of loss or destruction of data. There are also greater risks posed by information "in transit" (i.e., moving data between office and home).

The risks posed by working remotely can be summarised under three headings:

- Reputational: the loss of trust or damage to the Trust's relationship with its community;
- Personal: unauthorised loss of or access to data could expose staff or students to identity theft, fraud or significant distress; and
- Monetary: regulators such as the ICO can impose financial penalties and those damaged as a consequence of a data breach may seek redress through the courts.

Roles and Responsibilities

The decision as to whether to allow remote access in relation to any given role rests with management.

Any member of staff working remotely is responsible for ensuring that they work securely and protect both information and Trust-owned equipment from loss, damage or unauthorised access.

Managers are responsible for supporting staff adherence with this policy. Additional measures may be put in place by management to ensure the rules contained within this policy are adhered to (for example, monitoring or supervision).

Failure to comply with this policy may result in disciplinary action.

Key Principles of Homeworking

Staff working remotely must ensure that they work in a secure and authorised manner. This can be done by complying with the principles below: -

i. To adhere to the principles of the Data Protection Act 2018 and the Trust's Data Protection Policy in the same way as they would if they were working in one of our schools.

ii. Access to personal data must be controlled. This can be done through physical controls, such as locking the home office for physical data and locking the computer by using strong passwords (a mixture of letters, numbers and special characters).

iii. No other individuals should know or be able to guess your password(s). If passwords are written down (which should be a last case scenario) they must be stored securely (e.g., in a locked drawer or in a secure password protected database). Passwords should never be left on display for others to see.

iv. Automatic locks should be installed on IT equipment used to process Trust information that will activate after a period of inactivity (i.e., computers should automatically lock requiring you to sign back in after this period of time).

v. IT equipment used to process and store Trust information must be kept in a secure place where it cannot be easily accessed or stolen.

vi. Portable mobile devices (e.g. USB keys) are banned for use across the Trust, and staff must not use them to process and store Trust information.

vii. IT equipment used to process Trust information should not be used where it can be overseen by unauthorised persons.

viii. It is the responsibility of each member of staff to ensure that they are working in a safe environment. No health and safety risks must be taken when using this equipment.

ix. Access to certain systems and services by those working remotely are deliberately restricted and require additional authentication methods (two factor authentication, which requires an additional device to verify individuals). Any attempt to bypass these restrictions may lead to disciplinary action.

x. All personal information and in particular sensitive personal information should be encrypted/password protected before being sent by email where possible. Extra care must be taken when sending emails where auto-complete features are enabled (as this can lead to sending emails to similar/incorrect email addresses). The rules relating the sending of emails are outlined in the Trust's Acceptable Use Agreement.

xi. Staff should always use Trust/ school email addresses when contacting colleagues or students. If telephoning a child or parent at their home, staff should ensure that they use the Trust/ school telephone system (using the 3CX web or mobile app), or ensure their caller ID is blocked.

xii. Any technical problems (including but not limited to, hardware failures and software errors) which may occur on the systems must be reported to the Trust IT Support team via the Helpdesk immediately.

xiii. To adhere to the Trust's Data Retention Policy and ensure that information held remotely is managed according to the data retention schedule. Data should be securely deleted and destroyed once it is no longer needed.

xiv. If communicating remotely via video conferencing and social media, staff must adhere to using only those platforms which have been approved by the Trust and follow the Trust's guidance on the safe use of video conferencing.

xv. To be vigilant to phishing emails and unsafe links. If clicked these links could lead to malware infection, loss of data or identity theft. Staff should be particularly vigilant about emails that are flagged as coming from an external email address. The Trust also employs software to monitor and quarantine suspicious emails.

xvi. Staff should not access inappropriate websites on Trust devices or whilst accessing Trust networks.

xvii. Staff who have been provided with Trust-owned IT equipment to work remotely must:

a. only use the equipment for legitimate work purposes;

b. only install software on the equipment if authorised by the Trust's IT support team. Please note that this includes photos, video clips, games, music files and opening any documents or communications from unknown origins;

c. ensure that the equipment is well cared for and secure;

d. not allow non-staff members (including family, flatmates and friends) to use the equipment or to share log in passwords or access credentials with them;

e. not attempt to plug in memory sticks into the equipment;

f. not collect or distribute illegal material via the internet;

g. ensure anti-virus software is regularly updated; and

h. to return the equipment securely at the end of the remote working arrangement.

xviii. Staff who process Trust data on their own equipment are responsible for the security of the data and the devices generally and must follow the School's Bring Your Own Device Policy and Acceptable Use Policy. In particular:

a. Where possible, devices must be encrypted;

b. An appropriate passcode/password must be set for all accounts which give access to the device. Passwords must be of a complex nature (a mix of uppercase and lower case letters, numbers and special characters) and must not be shared with others;

c. The device must be configured to automatically lock after a period of inactivity (no more than 15 minutes);

d. Devices must remain up to date with security software (such as anti-virus software);

e. The theft or loss of a device must be reported to IT services just in the same way as if a Trust-owned device were lost;

f. Any use of privately-owned devices by others (family or friends) must be controlled in such a way as to ensure that they do not have access to Trust information. This will include emails, learning platforms and administrative systems such as Bromcom/ Sims;

g. Devices must not be left unattended where there is a significant risk of theft;

h. The amount of personal data stored on the device should be restricted and the storing of any sensitive data avoided;

i. Using open (unsecured) wireless networks should be avoided. Consider configuring your device not to connect automatically to unknown networks;

j. If the device needs to be repaired, ensure that the company used is subject to a contractual agreement which guarantees the secure handling of any data stored on the device;

k. Appropriate security must be obtained for all Trust information stored on the device (including back up arrangements) and there must be secure storage for any confidential information;

l. Care must be taken with file storage. Any Trust related work should be stored on Trust-provided storage, such as OneDrive, SharePoint or (where available) network drives. No Trust data should be stored on a home computer or on a storage device (such as USB stick);

m. The School may require access to a privately owned device when investigating policy breaches (for example, to investigate cyber bullying);

n. All data must be removed from privately-owned devices when it is no longer needed or at the request of the Trust; and

o. Devices must be disposed of securely when no longer required.

xix. Staff are responsible for ensuring the security of Trust property and all information, files, documents, data etc within their possession, including both paper and electronic material. In particular, physical data (i.e., paper documents, which includes documents printed off-site) must be secured and staff must ensure that:

a. Paper documents are not removed from the Trust without the prior permission of the Head of School or the Trust or School Data Protection Lead. When such permission is given, reasonable steps must be taken to ensure the confidentiality of the information is maintained during transit. In particular the information is not to be transported in see-through bags or other un-secured storage containers;

b. Paper documents should not be used in public places and not left unattended in any place where it is at risk (e.g., in car boots, in a luggage rack on public transport);

c. Paper documents taken home or printed off-site containing personal information, sensitive data and confidential information are not left around where they can be seen, accessed or removed;

d. Paper documents are collected from printers as soon as they are produced and not left where they can be casually read;

e. The master copy of the data is not to be removed from Trust premises;

f. Paper documents containing personal data are locked away in suitable facilities such as secure filing cabinets off-site just as they would be in our schools;

g. Documents containing confidential personal information are not pinned to noticeboards where other individuals may be able to view them; and

h. Paper documents are disposed of securely by shredding and should not be disposed of with the ordinary waste unless it has been shredded first.

xx. Any staff member provided with Trust devices must not do, cause or permit any act or omission which will avoid coverage under the Trust's insurance policy. If in any doubt as to whether particular acts or omissions will have this effect, the staff member should consult their line manager immediately.

xxi. All staff must report any loss or suspected loss, or any unauthorised disclosure or suspected unauthorised disclosure, of any Trust-owned IT equipment or data immediately to the Trust Network Manager and the Trust or School Data Protection Lead in order that appropriate steps may be taken quickly to protect School data. Failure to do so immediately may seriously compromise Trust security. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

Appendix A – Remote Working Data Protection Policy Summary

STOP working remotely if you are handling high risk/sensitive data:

- on a device without adequate protection (antivirus, encryption)
- in a public space (café, train)
- on public/unsecured WiFi connection
- without Trust authorisation

BEWARE

Of… printer-sharing, remote desktop file-sharing, remote USB connections

Due to an **increased risk of hackers** – This is not just about using devices or systems that are less secure, but also the risk of employees being duped into changing passwords or to download software that contains malware. Always be careful which websites you visit and which email attachments you open.

CAUTION working remotely:

- using personally owned devices (tablet, smartphone)
- using unknown WiFi connections

OK to work remotely:

- whilst on School premises/servers
- using a School owned device
- using a School owned device which is directly connected to the School network
- using a device and/or data which is encrypted.