Home Working Policy

The Oldershaw Academy

Approved by:	[Name]	**Date:**	
Last reviewed on:	[Date]		
Next review due by:	[Date]		

Home Working Policy

Scope and Definitions

This policy applies to all staff who work from home and/or use or access Academy systems or information from home or while working remotely. This includes individuals who are given access to the Academy networks and Academy 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 off the Academy site. This includes working while connected to the Academy's WiFi 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 from home presents both significant risks and benefits.

Staff may have remote access to information held on secure Academy servers, but without the physical protections available in school and the network protections provided by firewalls and access controls there are much greater risks of unauthorised access to, and 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 from home can be summarised under three headings:

- *Reputational:* the loss of trust or damage to the Academy'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 partial or full-time homeworking in relation to any given role rests with management.

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

Managers are responsible for supporting their staff's 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 from home 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 Academy's Data Protection Policy in the same way as they would if they were working in the Academy.

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 members of the household should know or can 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 other to see.

iv. Automatic locks should be installed on IT equipment used to process Academy 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 Academy information in the home must be kept in a secure place where it cannot be easily accessed or stolen.

vi. Portable mobile devices used to process and store Academy information should be encrypted where possible (or at least password/pin code protected) and should never be left unattended in a public place.

vii. IT equipment in the home used to process Academy 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 at home. No health and safety risks must be taken when using this equipment.

ix. Access to certain systems and services by those working from home or remotely may be deliberately restricted or may require additional authentication methods (such as two factor authentication using 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 to the sending of emails are outlined in the Academy's Electronic Information and Communications Systems Policy.

xi. Always use your Academy email address when contacting colleagues or students. If telephoning a child or parent at their home ensure that your 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 Network Manager immediately.

xiii. To adhere to the Academy's Data Retention policy and in particular ensure that information held remotely is managed according to the data retention schedule and 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 Academy and follow the Academy's guidance on the safe use of video conferencing.

xv. To be vigilant to phishing emails and not clicking on unsafe links. If clicked these links could lead to malware infection, loss of data or identity theft.

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

xvii. Staff who have been provided with Academy-owned IT equipment to work from home must:

a. only use the equipment for legitimate work purposes;

b. only install software on that equipment if authorised by the Academy's IT support. Please note that this includes screen savers, 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 unless encrypted and supplied by the Academy);

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 Academy data on their own equipment are responsible for the security of the data and the devices generally and must follow the Academy's Information Security Policy. In particular:

a. Devices must be encrypted where possible;

b. An appropriate passcode/password must be set for all accounts which give access to the device. Passwords must be complex (a mix of 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 an Academy-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 Academy information. This will include Academy emails, learning platforms and administrative systems such as SIMs;

g. Devices must not be left unattended where there is a significant risk to 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 Academy 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 Academy related work should be stored on the Academy network area. No Academy data should be stored on a home computer or on an un-encrypted storage device (such as USB stick);

m. The Academy 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 Academy; and

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

xix. Staff are responsible for ensuring the security of Academy 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 at home) must be secured and Staff must ensure that:

a. Paper documents are not removed from the Academy without the prior permission of the Principals. 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 at home 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 Academy premises;

f. Paper documents containing personal data are locked away in suitable facilities such as secure filing cabinets in the home just as they would be in the Academy;

g. documents containing confidential personal information are not pinned to noticeboards where other members of the household 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 Academy devices must not do, cause or permit any act or omission which will avoid coverage under the Academy'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 Academy-owned IT equipment to the Network Manager or data immediately to the Data Manager in order that appropriate steps may be taken quickly to protect Academy data. Failure to do so immediately may seriously compromise Academy security. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Manager who will liaise with the Data Protection Officer.

Links to Other Policies

- Electronic Information and Communications Systems Policy
- Information Security Policy
- Data Protection Policy

Appendix A: Homeworking Guidance Handout for Staff

STOP working from home or 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 School authorisation

BEWARE

- Home printer-sharing, remote desktop file-sharing, remote USB connections
- 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 from home or remotely

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

OK to work from home or 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.