



‘Innovative Education - Transforming Lives’

HOME AND REMOTE WORKING POLICY

Responsible Directors	Board of Directors
Responsible Persons	Mrs. B Nixon CEO
Date Policy Agreed	March 2020
Review Date	March 2021

Contents

Page

1	Introduction	3
2	Purpose and Objectives	3-4
3	Scope	4
4	Definition	4
5	Procedures and expectations	5
6	Health and Safety	5
7	Computer Equipment	5
8	IT Support	6
9	Expenses	6
10	Security	6

Version control

<i>Version</i>	<i>Revision Date</i>	<i>Revised by</i>	<i>Section Revised</i>
V1	New policy	L Burton	

1. Introduction

For the purpose of this policy, the term homeworking applies equally to remote and mobile working.

- 1.1 To enable the Trust/Academy to maximise its employee's effectiveness and productivity but at the same time giving more flexibility in their working lives, the Trust/Academy is committed to supporting homeworking.
- 1.2 To enable the Trust/Academy to continue with operational activities in emergency situations such as school closure due to fire, flood or illness.
- 1.3 The Trust/Academy, in support of homeworking, will provide the tools to reap the benefits of adopting flexible working practices that meet the needs of the business, the team and the individual. This will maximise our ability to provide the highest quality of service whilst at the same time managing our operating challenges.
- 1.4 The Trust/Academy will ensure that all users who work from home or remotely are aware of the acceptable use of portable computer devices and remote working opportunities. Portable computing devices are provided to assist users to conduct official business efficiently and effectively. This equipment and any information stored on it should be recognised as valuable organisational information and assets and as such should be safeguarded appropriately.
- 1.4 The Trust/Academy is committed to its duty to fulfill the requirements of the Equality Act 2010. Where reasonable adjustments are already made at an employee display screen workstation, such as ergonomic and/or personalised equipment, that same help, support and protection shall be afforded to homeworkers where appropriate.

2. Purpose and Objectives

The purpose of this policy is to establish the standards, working practices and supported configurations of remote working solutions.

- 2.1 The Trust/Academy's aim is to recruit and retain key personnel with the necessary skills and knowledge to assist in meeting its overall objectives. The Trust/Academy therefore supports homeworking where an employee's effectiveness, productivity and efficiency can be enhanced by working from home on specific projects, or for other specific reasons where possible and practical. Homeworking can also be a benefit to the employee allowing them to have flexibility for an equivalent or enhanced service to the Trust/Academy.
- 2.2 This Trust/Academy is committed to adopting a flexible approach to working arrangements and homeworking may, therefore, be part of the employees working pattern or may be carried out as and when required as is appropriate. Homeworking has a number of benefits for the employee and employer. The employee gains greater flexibility of working times, time and cost savings on commuting and can have a quieter work environment in which to undertake their

work. Homeworking must not be seen as an alternative to making usual Childcare/dependent/carer arrangements, any arrangements that the member of staff would require to have in place to enable him or her to attend the workplace must remain in place throughout the homeworker's hours of work unless previously agreed with the CEO/Principal.

3. Scope

- 3.1 It is appreciated that this concept may not be suitable for many types of work, but a wide range of posts can be considered for homeworking and in the case of an emergency would be expected to continue to work from home where possible. The one area not suited for homeworking is when the post requires a high element of continued face-to-face pupil contact.

4. Definition

- 4.1 Homeworking consists of working based at home rather than at the normal place of work and may involve using IT systems to perform work and to remain in contact with managers and employee. It is carried out to an agreed work pattern on a permanent, regular, part-time, temporary or ad hoc basis.
- 4.2 This policy should be adhered to at all times whenever any user makes use of portable computing devices. This policy applies to all users' use of the Trust/Academy IT equipment and personal IT equipment (where agreed in the first instance) when working on official Trust/Academy/ business away from the normal working premises.
- 4.3 The policy also applies to all users' use of Trust/Academy IT equipment and personal IT equipment (where agreed in the first instance) to access Trust/Academy information systems or information whilst outside the United Kingdom.
- 4.4 Portable computing devices include, but are not restricted to, the following:
- Laptop computers
 - Tablet/iPads
 - Mobile phones including Smart phones
 - Wireless technologies
- 4.5 For remote homeworking it is essential that those undertaking work from home are able to make available a room or area of their home for use as an office/working area. The employees work location, however, will remain at their normal place of work as included in the terms of their contract of employment.

5. Procedure and expectations

5.1 All employees should be able to demonstrate they can:

- Work independently and on their own initiative
- Motivate themselves
- Complete projects within set deadlines
- Manage workload effectively
- Cope well under any new pressure posed by working at home
- Adjust to new work practices
- Maintain contact with all affected by own work

5.2 Expectations of home working arrangements:

- Managers need to determine how work will be monitored, produced and delivered
- For home working to take place it must be established that the work to be completed can be done at home without regular/frequent face to face contact or direct supervision
- Home working arrangement must be reviewed termly

6. Health and Safety

6.1 All employees who work at home have duties under the Health and Safety at Work Act in the same way that they would otherwise have in the workplace provided that:

- It has been established that such working will not unreasonably impact on the employee's health and safety; and
- There are suitable facilities at the employee's home to effectively carry out the role; and
- Effective mechanisms for communication and support are in place
- Risk assessments must be undertaken for all home working and recorded on file
- All home working employees will be required to undertake a DSE assessment before commencing work

7. Computer Equipment

7.1 Equipment required to enable the employee to work effectively at home will be provided by the Trust/Academy i.e. laptop, mobile phone and items of stationery. This equipment will remain the property of the Trust/Academy and will vary from case to case. The employee must: -

- Take reasonable care of it
- Use it only for official purposes
- Use it only in accordance with any operating instructions

- Return it to the Trust/Academy when requested
- Use it in accordance with any existing Trust/Academy policies

If personal equipment is used for work purposes (agreed in the first instance) the Trust/Academy is not responsible for the maintenance, replacement or repair of any equipment used.

- 7.2 Special attention will be paid to any requirement to use or access information that is deemed OFFICIAL or SENSITIVE in accordance with the Trust/Academy Data Protection Policy and restrictions imposed under GDPR compliance.
- 7.3 If employees are required, to work from home on an ad hoc or short term basis, provision will be made for them to use a trust or academy laptop for the work to be undertaken. Employee's personal equipment must only be used in circumstances that have been agreed.

8. IT Support

- 8.1 IT Helpdesk support is still accessible for homeworkers by contacting the IT provider's helpdesk either by phone or email
- 8.2 Trust/Academy equipment experiencing issue will be repaired by Trust/academies IT services provider.
- 8.3 Multi Factor Authentication must be applied to homeworkers remotely dialing onto the Trust/Academy network systems to maintain security

9. Expenses

- 9.1 If the employee uses their own telephone line, charges for business calls (excluding line rental) will only be reimbursed if clearly identified on an itemised bill and agreed prior to use with the manager.
- 9.2 Stationery where required will be provided by the Trust/Academy, but employees should notify their line Manager of all stationery taken out of the office/academy.
- 9.3 Printing costs will not be reimbursed, any items for printing should be stored in a file on the computer and printed when next in the office/academy

10. Security

- 10.1 Employees are responsible for the security of all data, whether held on computer, encrypted memory sticks or paper and must ensure it is stored securely to maintain confidentiality of information from members of the family or visitors.

10.2 Sensitive material or personal data must be disposed of by recognised methods using office based shredding equipment or other means.

10.3 It is the user's responsibility to ensure that the following points are adhered to at all times:

- Users must take due care and attention of portable computer devices when moving between work, home or any other business site
- Due to the high incidence of car thefts laptops or other portable equipment must never be left unattended in cars or taken into vulnerable areas.
- Users will not install or update any software onto a Trust/Academy owned portable computer device
- Users will not install any screen savers onto a Trust/Academy owned portable computer device
- Where a wireless connection is used, this should be a secure connection.
- Users will not install any hardware to or inside any Trust/Academy owned portable computer device, unless authorised by the council's IT Services
- Users will inform the IT Services Helpdesk of any Trust/Academy owned portable computer device message relating to configuration changes
- Business critical data should be stored on a Trust/Academy network drive and not held on the portable computer device
- All faults must be reported to the IT Service Helpdesk (helpdesk@theacsgroup.co.uk)
- Users must not remove or deface any asset registration number
- No family members may use any Trust/Academy provided equipment. The Trust/Academy provided equipment is supplied for the staff members' sole use
- The user must ensure that reasonable care is taken of the Trust/Academy equipment supplied
- The user should seek advice from the Trust/Academy before taking any equipment outside the United Kingdom. The equipment may not be covered by the Trust/Academy's normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel
- The Trust/Academy may at any time, and without notice, request a software and hardware audit and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit
- Any user who undertakes work at home or remotely in relation to their official duties using their own IT equipment must understand that they are not permitted to hold any database, or carry out any processing of OFFICIAL or SENSITIVE information relating to the Trust/Academy, its employees. Pupils or suppliers.
- Any user accessing, or using OFFICIAL or SENSITIVE information, must only use Trust/Academy owned equipment which has appropriate technical security and advanced authentication mechanisms whilst working remotely.

- 10.4 Users should be aware of the physical security dangers and risk associated with working within any remote office or mobile working location.
- 10.5 Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. For home working it is recommended that the office area of the house should be kept separate from the rest of the house where possible. Equipment must be secured whenever it is not in use by either locking away in a cupboard or drawer.
- 10.6 Users must ensure that access/authentication and personal identification numbers are kept in a separate location to the portable computer device at all times. Removable media devices and paper documentation must not be stored with the portable computer device. Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities when not in use. Documents should be collected from printers as soon as they are produced and not left where they can be casually read. Waste paper containing OFFICIAL or SENSITIVE information must be shredded to required standards
- 10.7 IT Services will provide up-to-date Anti-Virus software to all Trust/Academy equipment. Users who work remotely must ensure that their portable computer devices are connected to internet at least once every two weeks to enable the Anti-Virus software to be updated.
- 10.8 Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes. All data on portable computer devices must, where possible, be encrypted. If this is not possible, then all OFFICIAL or SENSITIVE data held on the portable device must be encrypted.

Policy Agreed: 16th September 2020

Signed CEO: 

Signed: Chair of Directors: 

Policy to be reviewed in March 2021