**Ravensbury Community School**



**Home Working Policy**

|  |  |  |
| --- | --- | --- |
| **Document Title: Home Working Policy**  **Document Owner: Ravensbury Community School**  **Review Date: September 2023**  **This policy will be reviewed annually unless an incident or new legislation or guidance suggest the need for an interim review.** | | |
| **Review Date** | **Changes Made** | **By Whom** |
| **September 2020** |  | **Headteacher** |
|  |  |  |
|  |  |  |

**Contents**

1 Managing the policy  
2 Introduction  
3 Purpose and objectives  
4 Scope  
5 Two tier system  
6 Definition  
7 Health and safety  
8 Computer equipment  
9 IT support  
10 Telephone  
11 Other expenses  
12 Security  
13 Hours worked

**1. MANAGING THE POLICY**

1.1  Compliance

All staff at Ravensbury Community School must comply with this policy.

Anyone who is found to have breached this policy could be subject to the School’s discipline policy and serious breaches of this policy could be regarded as gross misconduct.

If you do not understand the implications of this or how it may apply to you, seek advice from the Headteacher.

1.2  Equality and Diversity

Every policy must consider equality and identify any potential barriers or discrimination faced by people protected by equality legislation.

**2 INTRODUCTION**

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

2.2  Ravensbury Community School is committed to supporting homeworking where the situation calls for staff working from home.

2.3  We 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 in accordance with the School’s Staff IT Acceptable Use Policy. Portable computing devices, if provided, are to assist users to conduct official school business efficiently and effectively. This equipment and any information stored on it should be recognised as valuable organisational information assets and safeguarded appropriately in accordance with the School’s Data Protection Policy and Confidentiality Policy.

2.4  Ravensbury Community School is committed to its duty to fulfil 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.

**3 PURPOSE AND OBJECTIVES**

3.1  The purpose of this policy is to establish the standards, working practices and supported configurations of remote working solutions as the situation calls for. This includes any large scale incident that requires school closures either as a government directed closure or as a result of large scale damage to a school building.

3.2  The School is committed to adopting a flexible approach to working arrangements and homeworking 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/dependant/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.

**4 SCOPE**

4.1  This policy applies to all school staff who have access to school information, information systems or IT equipment.

**5 TWO TIER SYSTEM**

5.1 This policy is split into two separate categories:

**Hot Desking**

* Where the employee wishes to work at home on an ad hoc basis, which is to the benefit to the employee allowing flexibility and meets the business needs, whilst also minimising the need for on-site accommodation

**Home or Remote Working**

* Employees who may apply under the Flexible Working Regulations, to work from home ;
* Staff, who as a result of serious incident such as school closure, are required to work from home.

**6 DEFINITION**

6.1  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 School’s IT equipment and personal IT equipment when working on official School business away from the School’s premises (ie working remotely).

6.2  The policy also applies to all users’ use of School IT equipment and personal IT equipment to access school information systems or information whilst outside the United Kingdom.

6.3  Portable computing devices include, but are not restricted to, the following:

* Laptop computers
* Tablet PCs
* Mobile phones inc Smart phones
* Wireless technologies

6.4  **For both Hot Desking and 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 the school as included in the terms of their contract of employment.

**7 HEALTH AND SAFETY**

7.1 All employees who work at home have duties under the Health and Safety at Work Act in the same way as other employees. Where the employee is only working from home on an ad hoc basis the employee may carry out a self-assessment at home. Managers will be responsible for ensuring appropriate risk assessments are undertaken.

**8 COMPUTER EQUIPMENT**

8.1  There are several IT solutions to achieving a suitable working from home environment. The solution installed will largely depend on the type and quantity of work that the employee will be undertaking at home. This decision will be made in consultation between IT and the Headteacher, in accordance with the budget of the school.

8.2  Special attention will be paid to any requirement to use or access information that is deemed personal or sensitive under the Data Protection Act 2018. (See the school’s data protection policy).

8.3  In certain circumstances it may not be technically feasible to provide the IT facilities required for an employee to carry out their role effectively from home. In these instances the Headteacher will be advised by the IT Lead in liaison with the employee.

8.4 It is understood that staff at times make use of personal devices which are not School owned/managed to access the School’s IT systems. To help ensure that School data has the appropriate protective measures in place, it is now policy that any personal device used to access School IT systems has the minimum security measurements in place to assist in data integrity – Please see the School Staff IT Acceptable Use Policy.

8.5 Unless a school telephone has been provided, the employee will be required to use their own telephone for making occasional telephone calls while working from home. They must withhold their number if making contact with parents. If speaking with children always request to be on speaker phone.

**9 IT SUPPORT**

9.1 School equipment will be maintained by the School. If the employee uses their own personal mobile equipment, they will be responsible for any repairs or technical support.

**10 OTHER EXPENSES**

10.1 If the employee has requested to work from home, expenses for heating, lighting etc., will not be reimbursed.

10.2  Stationery will be provided by the school, but employees should notify their line manager of all stationery taken out of the office.

**11 SECURITY**

When working from home, the employee must be aware of the increased risk of a security breach.

11.1  All School policies must be complied with at all times

11.2  For both Hot Desking and Homeworking, employees are responsible for the security of all data, whether held on IT equipment or paper and must ensure it is stored securely to maintain confidentiality of information from members of the family or visitors.

11.3  Sensitive material or personal data must be disposed of by recognised methods using office based Shred-it bins. Further information on data protection is held within the School’s data protection policy.

11.4  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 and personal mobile devices when moving between home and another business site.
* Due to the high incidence of car thefts, laptops or other portable equipment where possible, should not be left unattended in cars or taken into vulnerable areas.
* Users will not install or update any software onto a School owned portable device.
* Users should connect with a wired connection wherever possible. Where a wired connection is not possible and a wireless connection is used, this should be a secure connection.
* Users will not install any hardware on or inside any school owned portable computer device, unless authorised by the School’s IT Lead.
* Users will allow the installation and maintenance of the School’s installed Anti-Virus updates immediately.
* Users will inform the IT Lead of any School owned portable computer device message relating to configuration changes.
* Business critical data should be stored on a school network drive and not held on the portable computer device
* All faults must be reported to the IT Lead.
* Any equipment used at home is subject an electrical safety inspection on an annual basis
* Users must not remove or deface any asset registration number
* User requests for upgrades of hardware or software must be approved by the IT Lead with financial authorisation. Equipment and software will then be purchased and installed by the IT Lead.
* No family members may use any School provided equipment. The School provided equipment is supplied for the staff members’ sole use
* The user must ensure that reasonable care is taken of the School equipment supplied
* The user should seek authorisation from the Headteacher before taking any School supplied equipment outside the United Kingdom. The equipment may not be covered by the School’s normal insurance against loss or theft and the equipment is liable to be confiscated by Airport Security personnel
* The School 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
* Under no circumstances should personal, or sensitive information be emailed to a private non- school email address. For further information, please refer to the school’s Staff IT Acceptable Use Policy
* All breaches should be reported to the school and to Global Policing as soon as possible, so we can ensure the processes of working at home remain robust.
* Ensure that screens are locked when not at use - even at home.

11.5 Equipment must be kept physically secure in accordance with this policy to be covered

for insurance purposes. When travelling by car, best practice is to place the laptop the

boot of your car before starting your journey and avoid any unnecessary stops eg

the supermarket etc.

11.6 In areas where there are likely to be members of the general public, portable or mobile

ICT equipment must not be left unattended and, wherever possible, must be kept out

of sight.

11.7 Portable equipment must be transported in its protective case supplied.

**12 REMOTE AND MOBILE WORKING ARRANGEMENTS**

12.1 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. Equipment must be secured whenever it is not in use by either locking away in a cupboard or drawer or by locking the device to the desk

12.2 Users must ensure that access/authentication codes 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 (eg secure filing cabinets) 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 personal or sensitive information must be disposed of in the on-site Shred-it bins.

12.3 Anti Virus Protection - The IT Manager will deploy an up-to-date Anti Virus signature file to all users who work away from School premises. Users who work remotely must ensure that their portable computer devices are connected to the school network at least once every two weeks to enable the Anti Virus software to be updated.

12.4 Access Controls - It is essential that access to all personal or sensitive information is controlled. This can be done through physical controls, such as locking the home office or locking the computer’s keyboard. Alternatively, or in addition, this should be done logically such as by password or user login controls.

12.5  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 personal or sensitive data held on the portable device must be encrypted in accordance with the School Staff IT Acceptable Use Policy. A sufficiently secure remote access mechanism must be configured to allow remote users access to school systems if connecting over Public Networks, such as the Internet.

12.6 Staff may be asked to undertake the live streaming of lessons using a platform which has been assessed for data protection and privacy compliance. Staff should position their camera against a neutral background; such that nothing which could identify where the member of staff lives.

**13 HOURS WORKED**

13.1 Working hours will be communicated to staff in the event they are required to work from home.