Model Schools Home & Mobile Working Policy

Author:	Lee Gardiner
Owner:	Senior IG Officer (Schools DPO)
Version Number:	v1.1
Date of Issue:	23/07/24

1 PURPOSE

1.1 St Anne's R.C. Primary School provides users with the facilities and opportunities to work remotely as appropriate. The purpose of this document is to define the Remote Working policy for St Anne's R.C. Primary School.

1.2 Portable computing devices are provided 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 they should be safeguarded appropriately.

2 Scope

2.1 This policy applies to all School Staff, including teaching and support staff, who are permitted to work from away from the office.

2.2 It is the responsibility of the SBM, Office Manager and Head Teacher to exercise appropriate controls to minimise the risk of misuse and to report misuse if it occurs.

2.3 Portable computing devices include, but may not be limited to, the following:-

Laptop computers
Tablet PCs
Mobile Phones
USB Pen Drives
Wireless technology products.

2.4 The School is not responsible for supporting any equipment that is not owned by the School and procured through the appropriate channels. Any support provided to the users of such devices, will be provided on a best efforts basis only.

3 Eligibility

3.1 There is no automatic entitlement to work from home. Head Teachers will determine whether home working is appropriate on a case by case basis.

3.2 The majority of remote workers will already be supplied with an appropriate School owned portable device. Users who do not have an appropriate portable device can request that they are provided with an appropriate school owned device.

3.3 An employee wishing to work from home must first of all gain the approval of the Head Teacher, or in the case of the Head Teacher, the Chair of Governors

3.4 Once approval has been granted the schools will follows its standard process for providing remote access to its network.

4 Risk

4.1 St Anne's R.C. Primary School recognises mobile computing increases risk for the School because mobile computing devices are small, valuable, can be removed quickly, are easily hidden, and there is a market for them. To mitigate the risk of information loss, all School computers, will be encrypted to protect the information on the device, or in the case of smartphones and some tablets, the device is managed using appropriate applications such as the Microsoft Outlook Email app.

4.2 Securing PROTECT or RESTRICTED data when users work remotely or beyond the School network is a pressing issue. Particularly in relation to the Council's need as an organisation to protect data in line with the requirements of GDPR and the Data Protection Act 2018.

4.3 This policy aims to mitigate the following risks:-

4.3.1 increased risk of equipment damage, loss or theft.
4.3.2 accidental or deliberate overlooking by unauthorised individuals.
4.3.3 Unauthorised access to CLASSIFIED data, PROTECT and RESTRICTED information.
4.3.4 potential sanctions against the School or Individuals imposed by the Information Commissioner's Officer as a result of information loss or misuse.
4.3.5 potential legal action against the School or individuals as a result of information loss or misuse.
4.3.6 School reputational damage as a result of information loss or misuse.

4.4 Non-compliance with this policy could have a significant effect on the efficient operation of the School and may result in financial loss and an inability to provide necessary services to our staff, pupils, parents and partners.

5 Applying the Policy

5.1 All IT equipment (including portable computer devices) supplied to users is the property of St Anne's R.C. Primary School, and must be returned upon the request of the School.

5.2 Access for St Anne's R.C. Primary School staff or other authorised individuals of St Anne's R.C. Primary School shall be given to allow essential maintenance security work or removal, upon request.

5.3 All IT equipment should be supplied and installed by authorised staff. All hardware and software should only be provided by St Anne's R.C. Primary School unless access to networks is available remotely.

5.4 Where St Anne's R.C. Primary School allows staff to use their own devices, particularly for access to email, staff should only use the appropriate Microsoft Outlook App for their device which should be appropriately secured to prevent unauthorised access.

This includes securing the device itself using the appropriate secure access requirements built into the device's operating system. This can include, but is not limited to, the use of access codes, facial recognition or other biometric measures.

5.5 Where users access School services from their own equipment it is a requirement that the user ensures that antivirus protection software is installed and up to date on their device(s).

6 Users responsibilities

6.1 It is the user's responsibilities at all times, whether working on School premises or remotely, to follow the School IT Policy to ensure that the following points are adhered to at all times:-

6.1.1 Users must take due care and attention of portable computer devices when moving between school, home and other sites.

6.1.2 Users will not install or update any software on to a School owned portable computer device.

6.1.3 Users will not install any screen savers on to a School owned portable computer devices and will not disable any screen saver in use.

6.1.4 Users will not change the configuration of any School owned portable computer device.

6.1.5 Users will not install any hardware to or inside any School owned portable computer device, unless authorised by SLT.

6.1.6 Users will allow, and assist if necessary, the installation and maintenance of installed Anti Virus and Windows updates immediately, and any other software update required to protect the user and portable computer.

6.1.7 Users must inform the SBM/School IT Support (Delete/amend as necessary) of any School owned portable computer device message relating to configuration changes.

6.1.8 Business critical data should be stored on the School's network drive(s) and not held on the portable device.

6.1.9 All faults must be reported to the (Insert details of school IT Support Service).

6.1.10 Users must not removed or deface any asset registration number.

6.1.11 User registration must be requested through the request process. Any request must state which applications or system the user requires access to.

6.1.12 No family members, relatives or any other non-School Staff may use School owned IT equipment. St Anne's R.C. Primary School owned and supplied IT equipment is supplied for use by School staff only. Staff should ensure apps on personal devices are appropriately secured to prevent unauthorised access should that device be used by a third party i.e. Password Protection to access Outlook email client

6.1.13 Users must seek to prevent the inadvertent disclosure of any School information, by avoiding being overlooked when working and by taking care when using School information i.e. by carefully checking the email distribution list for any material to be transmitted.

6.1.14 Users should seek advice and approval from SLT/Governors 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.

6.1.15 St Anne's R.C. Primary School may at any time, and without notice, request or be required to carry out a software and hardware audit. There may be a requirement to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.

6.1.16 Any user who chooses to undertake 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 information relating to the School, staff, pupils,

parents and partners on that device and information should be accessed from and saved to the appropriate School network location

6.1.17 Caution should be exercised when emailing personal information.

6.1.18 Users must ensure that antivirus software on their own devices is up to date.

7 Remote and mobile working arrangements

7.1 Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

7.2 Equipment should not be left unattended or left where it may attract the interest of the opportunist thief. In the home it should 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. Monitors or other displays should also be positioned to avoid overlooking, including not being viewable through a window.

7.3 Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities such as a secure filing cabinets when not in use. Waste paper containing School or personal information must be shredded to required standards.

8 Access controls

8.1 It is essential that access to all School or personal information is controlled. This can be done through physical controls, such as locking the home office or locking the device. Alternatively, or in addition all School Devices will return to the login screen following the screen saver being displayed.

8.2 Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

8.3 All data on portable computer devices must be encrypted. If this is not possible then all School or personal data held on the portable devices must be encrypted.

8.4 Access to the Internet from School owned IT equipment will only be allowed via connection to the School's provided system and not directly to the Internet.

8.5 All documents must be produced and stored in compliance with the School's Records Management Policy

9 Anti virus protection

9.1 School IT will deploy an up to date anti virus signature files to all users who work away from the School's 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 fully updated.

10 Key messages

10.1 It is the user's responsibility to use portable computer devices in an acceptable way. This includes not installing software, taking due care and attention when moving portable computer devices and not emailing Personal information to a non-Council email address if a more secure alternative is available. This may include encrypted email services such as Egress.

10.2 Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

10.3 It is the user's responsibility to ensure that access to all information is controlled i.e. through password controls.

10.4 All portable devices should be encrypted/secured appropriately.