**Document Owner and Approval**

The Bridges Federation is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the School’s policy review schedule.

A current version of this document is available to all members of staff on the Google staff drive .

Signature: Date: July 2024

**Version History Log**

|  |  |  |
| --- | --- | --- |
| **Version** | **Description of Change** | **Date of Policy Release by Judicium** |
| 1 | Initial Issue | April 2020 |
| 2 | Formatting amendments | 02.08.22 |

**Home Working and Personal Devices Policy**

**Scope and Definitions**

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

Staff may have remote access to information held on secure School servers but without the physical protections available in 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 from home can be summarised under three headings:

* Reputational: the loss of trust or damage to the School’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 penaltiesand 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 School-owned equipment from loss, damage or unauthorised access.

Managers are responsible for supporting staff to 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: -

1. To adhere to the principles of the Data Protection Act 2018 and the School’s Data Protection Policy in the same way as they would if they were working in School.
2. 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).
3. No other members of the household 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.
4. Automatic locks should be installed on IT equipment used to process School 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).
5. IT equipment used to process and store School information in the home must be kept in a secure place where it cannot be easily accessed or stolen.
6. Portable mobile devices used to process and store School information should be encrypted where possible (or at least password/pin code protected) and should never be left unattended in a public place.
7. IT equipment in the home used to process School information should not be used where it can be overseen by unauthorised persons.
8. 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.
9. 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 which requires an additional device to verify individuals). Any attempt to bypass these restrictions may lead to disciplinary action.
10. 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 School’s Acceptable Use Agreement.
11. Staff should always use school email addresses when contacting colleagues or students. If telephoning a child or parent at their home, staff should ensure that their caller ID is blocked.
12. Any technical problems (including but not limited to, hardware failures and software errors) which may occur on the systems must be reported immediately.
13. To adhere to the School’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.
14. If communicating remotely via video conferencing and social media, staff must adhere to using only those platforms which have been approved by the School and follow the School’s guidance on the safe use of video conferencing.
15. To be vigilant to phishing emails and unsafe links. If clicked these links could lead to malware infection, loss of data or identity theft.
16. Staff should not access inappropriate websites on School devices or whilst accessing School networks.
17. If staff use the School device for personal use this must be in line with all guidance outlined in this policy.
18. Staff who have been provided with School-owned IT equipment to work from home must:
19. Sign our device loan agreement annually and agree to abide by all restrictions and guidance noted;
20. only use the equipment for legitimate work purposes;
21. only install software on the equipment if authorised by the School’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;
22. ensure that the equipment is well cared for and secure;
23. 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;
24. not attempt to plug in memory sticks into the equipment unless encrypted and supplied by the School);
25. not collect or distribute illegal material via the internet;
26. bring the school laptop into school once a year to ensure all updates are carried out and a check of the search history will be carried out and logged;
27. ensure anti-virus software is regularly updated; and
28. to return the equipment securely at the end of the remote working arrangement.

 xviii. Staff are responsible for ensuring the security of School 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:

1. Paper documents are not removed from the School without the prior permission from the LT. 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;
2. 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);
3. 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;
4. Paper documents are collected from printers as soon as they are produced and not left where they can be casually read;
5. The master copy of the data is not to be removed from School premises;
6. 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 School;
7. Documents containing confidential personal information are not pinned to noticeboards where other members of the household may be able to view them; and
8. Paper documents are disposed of securely by shredding and should not be disposed of with the ordinary waste unless it has been shredded first.

xix. Any staff member provided with School devices must not do, cause or permit any act or omission which will avoid coverage under the School’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.

xx. All staff must report any loss or suspected loss, or any unauthorised disclosure or suspected unauthorised disclosure, of any School-owned IT equipment or data immediately to the LT in order that appropriate steps may be taken quickly to protect School data. Failure to do so immediately may seriously compromise School 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).

**Using Your Own Device**

All staff should be using school devices as provided. There may be an occasion where personal devices are used for school work.

By accessing the School’s systems and networks, it is likely that staff will use personal data and so must abide by the terms of the Data Protection Act 2018 when doing so (including ensuring adequate security of that personal information).

Staff who process School data on their own equipment are responsible for the security of the data and the devices generally.

All employees must agree to the following terms and conditions in order to be able to connect their devices to the company network [and must follow the School’s Acceptable Use Policy]:

* When in School, staff should connect their device via the School’s wireless network for security.
* When out of School, staff should access work systems on their mobile device using Cisco anyconnect Remote Access or Google Drive.
* All internet access via the network is logged and as set out in the Acceptable Use policy, employees are blocked from accessing certain websites whilst connected to the School network.
* The use of camera, microphone and/or video capabilities are prohibited whilst in School unless this has been approved by the LT. If approved, any pictures, videos or sound recordings can only be used for School purposes and cannot be posted or uploaded to any website or system outside of the School network.
* You must not use your device to take pictures/video/recordings of other individuals without their advance written permission to do so.
* WhatsApp must not be used on personal devices for School related communication. Members of staff are able to use WhatsApp on their own devices for personal communication. However, staff should not communicate internally with other staff members for School business using their personal WhatsApp accounts, sharing School related information which could include categories of personal data.
* Where possible, devices must be encrypted;
* 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 letters, numbers and special characters) and must not be shared with others;
* The device must be configured to automatically lock after a period of inactivity (no more than 15 minutes);
* Devices must remain up to date with security software (such as anti-virus software); and the latest OS available for the device
* The theft or loss of a device must be reported to IT services just in the same way as if a School-owned device were lost;
* 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 School information. This will include school emails, learning platforms and administrative systems such as SIMS;
* Devices must not be left unattended where there is a significant risk to theft;
* The amount of personal data stored on the device should be restricted and the storing of any sensitive data avoided;
* Using open (unsecured) wireless networks should be avoided. Consider configuring your device not to connect automatically to unknown networks;
* 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;
* Appropriate security must be obtained for all School information stored on the device (including back up arrangements) and there must be secure storage for any confidential information;
* Care must be taken with file storage. Any school related work should be stored on the School network area. No school data should be stored on a home computer or on an un-encrypted storage device (such as USB stick);
* The School may require access to a privately owned device when investigating policy breaches (for example, to investigate cyber bullying);
* All data must be removed from privately-owned devices when it is no longer needed or at the request of the School; and
* Devices must be disposed of securely when no longer required.

**Non-acceptable Use**

* Any apps or software which are downloaded onto the user’s device whilst using the School’s own network is done at the users risk and not with the approval of the School.
* Devices may not be used at any time to:
* Store or transmit illicit materials;
* Store or transmit proprietary information belonging to the School;
* Harass others;
* Act in any way against the School’s Acceptable Use policy and other safeguarding and data related policies.
* Technical support is not provided by the School on the user’s own devices.

**Security**

* In order to prevent unauthorised access, devices must be password/pin/fingerprint protected using the features of the device and a strong password is required to access the School network.
* When using a web browser to access school information such as email or Google staff must never allow the browser to save the password on the device.
* When using personal data, it is the user’s responsibility to ensure they keep data secure on their device. This includes preventing theft and loss of data (for example, through password protection and cloud back up), keeping information confidential (for example, by ensuring access to emails or sensitive information is password protected) and maintaining that information.
* The School does not accept responsibility for any loss or damage to the user’s device when used on the School’s premises. It is up to the user to ensure they have their own protection on their own device (such as insurance).
* Staff are prevented from installing email apps which allow direct access to School emails without use of a login/password. This can be the passcode/fingerprint/face ID on a personal phone.
* If information is particularly sensitive then users should ensure that the data is either appropriately secured or deleted from the device (including from any local copies which may have been stored on the device.
* In the event of any loss or theft of personal data, this must be reported immediately as a data breach in accordance with the School’s Data Breach policy.
* The School may require access to a device when investigating policy breaches (for example, to investigate cyber bullying).
* Staff are not permitted to share access details to the School’s network or Wi-Fi password with anyone else.

All staff who wish to use their own devices to access the School’s network must sign and return the statement at the conclusion of this policy.

**Appendix A – Homeworking Guidance Handout for Staff**

**Device loan agreement staff**

**1. This agreement is between:**

1) Tower Bridge Primary School (“the school”)

2) [Name of staff member and their address] (“staff member” and “I”)

And governs the use and care of devices assigned to the staff member. This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school’s policies.

1. The school is lending the staff member a laptop (“the equipment”) for the purpose of doing school work from home.

2. This agreement sets the conditions for taking a Tower Bridge Primary School laptop (“the equipment”)]
home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I will adhere to the terms of loan.

I confirm that I have read, understood and will comply with the terms of the Home Working and Personal Devices Policy.

Staff are expected to use School owned and privately owned devices in an ethical manner at all times and adhere to the School’s policy as outlined above.

The School reserves the right to disconnect devices or disable services or access to services without notification.

The School will not monitor the content of the user’s own device but will monitor any traffic over the School system to prevent threats to the School’s network.

The employee is expected to use his or her devices in an ethical manner at all times and adhere to the School’s Home Working and Personal Devices policy.

The employee is personally liable for all costs associated with his or her device.

The School reserves the right to take appropriate disciplinary action up to and including summary dismissal for non-compliance with this policy.

**2. Damage/loss**

By signing this agreement I agree to take full responsibility for the loan equipment issued to me and I understand the conditions of the agreement.

I understand that I am responsible for the equipment at all times whether on the school’s property or not.

If the equipment is damaged, lost or stolen, I will immediately inform the school office and the school leadership team, and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

If there are any problems with software and I am unable to use the equipment, I will contact the school office immediately.

I agree to keep the equipment in good condition and to return it to the school on their demand in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure I take the following measures to protect the device:

* Ensure that access to the device is password protected
* Keep the device in a secure place when not in use
* Don’t leave the device in a car or on show at home
* Don’t eat or drink around the device
* Don’t lend the device to others or allow others to use the device, including family members
* Don’t leave the equipment unsupervised in unsecured areas
* Don’t stick or write anything on the device

**3. Unacceptable use**

I am aware that the school monitors the activity on this device.

I will be required to bring the laptop into school annually for a filtering and monitoring check that will look at my search history.

I agree that I will not carry out any activity that constitutes ‘unacceptable use’.

This includes, but is not limited to the following:

* Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
* Any illegal conduct, or statements which are deemed to be advocating illegal activity
* Activity which defames or disparages the school, or risks bringing the school into disrepute
* Causing intentional damage to ICT facilities or materials
* Using inappropriate or offensive language
* Using inappropriate programs or visiting inappropriate websites

I accept that the school will take action if I engage in any of the above **at any time.**

**4. Personal use**

I agree that I will use this device for educational purposes and appropriate personal use as agreed above and will not allow anyone else, including family members to use this device.

**5. Data protection**

The equipment is configured and maintained by @thebridgesfederation.org.uk G Suite platform.

I agree to take the following measures to keep the data on the device protected.

* Make sure the device is password protected.
* Make sure I lock the equipment if it’s left inactive for a period of time
* Do not share the equipment among family or friends

If I need help doing any of the above, I will contact the school office on the email
office@towerbridge.southwark.sch.uk or the Leadership Team.

**6. Return date**

I will return the device in its original condition to the school office when requested.

I will ensure the return of the equipment to the school if I am no longer employed by the federation.

**7. Consent**

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

|  |  |
| --- | --- |
| EMPLOYEE’S FULL NAME  |  |
| EMPLOYEE’S SIGNATURE |  |

**8. Equipment Details**

**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** Of… home 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 from home or remotely:

* using personally owned devices (tablet, smartphone)
* using unknown WiFi connections
* using school devices for personal use

**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.