(i)

St Hilary's School
Remote working: Mobile Device Policy

1. Introduction

1.1. Coronavirus (Covid-19) is causing unprecedented and fast moving changes to our ways of working. The Government is asking all employers, including schools, to consider how they can facilitate as much home working from employees as possible during this period. Many staff have been asked to work from home (partly or wholly) where their role permits this. As such, staff are being required to use mobile devices for work purposes (whether those devices are owned personally or by the School).

We actively promote democracy, the rule of the law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs. These are fundamental British Values which underpin all that we offer, as does our School Moto 'Not for oneself but for all.'

1.2. The aim of this policy is to support staff that are using mobile devices remotely for work purposes (whether owned personally or by the School) particularly during the Covid-19 outbreak. It ensures that staff are aware of:

1.2.1. the risks associated with using mobile devices remotely in terms of the security of St Hilary's IT resources and systems, and

1.2.2. the steps that must be taken to comply with St Hilary's legal obligations and protect personal data and confidential and proprietary information of the School.

2. Scope of this Policy

(i)

2.1. This policy covers all staff working remotely from home (including, employees, casual workers, volunteers, Governors and agency workers. All staff must be familiar with this policy and comply with its terms. It does not form part of any contractual arrangements with staff and the School reserves the right to amend and remove it at any time.

2.2. This policy applies to all devices used to access St Hilary's IT resources and systems (collectively referred to as **systems** in this policy), which may include (but are not limited to) smartphones, mobile or cellular phones, tablets, and laptop or notebook computers including any accompanying software or hardware (collectively referred to as a **device** in this policy).

2.3. A **work device** means any device that has been purchased, is owned or leased by the School (regardless of the source of funding). **Personally owned devices** means any device that is held personally by staff in a private capacity.

2.4. This policy supplements, and should be read in conjunction with, the School's other policies and procedures, including without limitation our Computing policy, Flexible Working policy, ICT Usage including Photograph and Mobile Phone policy for all staff, Document Retention policy, Privacy Notice and other IT related policies, which are available on the X drive. At the present time, these policies are reviewed and updated frequently and staff should refer to the very latest version of these policies.

2.5. All staff are responsible for the success of this policy. Any misuse (or suspected misuse) of a device or breach of this policy should be reported to the Deputy Head.

2.6. If you have any questions regarding this policy or have questions about using a device for remote working purposes, please contact the Deputy Head.

2.7. Staff must sign and return the declaration at the end of this policy to the Deputy Head.

3. Purpose of this policy

3.1 When you access our systems, you will be able to access data about the School, its employees, pupils, their parents, suppliers and other contacts, including information which

(i)

is confidential, personal or private. The definition of data is very broad, and includes all written, spoken and electronic information held, used, transmitted or otherwise processed by us or on our behalf, in whatever form (collectively referred to as **school data** in this policy).

3.2 When you access our systems remotely using a device (whether personal or a work device), St Hilary's are exposed to a number of risks, including the loss or theft of the device (which could result in unauthorised access to our systems or school data), the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device) and the loss or unauthorised alteration of or access to school data (including personal and confidential information which could expose the School to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy). Such risks could result in damage to St Hilary's systems and reputation. It could also seriously and irreparably damage the relationship between the School and its staff, parents and pupils all of whom have entrusted the School with their personal and sometimes highly sensitive information.

3.3 The purpose of this policy is to protect our systems and school data, and to prevent school data from being deliberately or inadvertently lost, disclosed, accessed or altered, while enabling you to access our systems using a personal or work device. This policy also sets out the circumstances in which we may monitor your use of our systems, access a device and retrieve, remove or destroy data on it and the action which we will take in respect of breaches of this policy. More information about how we monitor, record and process your personal data is contained in our separate Privacy Notice and Document Retention policy.

3.4 Any breach of this policy may lead to us revoking your access to our systems, whether through a personal or work device or otherwise. For employees, it may also result in disciplinary action up to, and including, dismissal and in the case of a breach of this policy by a casual or agency worker, the termination of the engagement. Disciplinary action may be taken whether the breach is committed during or outside hours or work. You are required to co-operate with any investigation into a suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.

(i)

4. Connecting to our systems

4.1. To access the School's systems on a device, you must have an Internet connection.

4.2. To access the remote system, personal login credentials should be used.

4.3. **Connecting a personal device to our systems**

4.3.1. Before using a personal device to connect to our systems, or to access school data, in accordance with this policy, you must:

4.3.2.1 register your device with the IT Department and seek approval to use the device for work purposes; and

4.3.2.2 implement such technical security measures as the IT Department may reasonably require.

4.3.2 You are not permitted to use any devices other than those that have been registered and approved by the School.

4.3.3 In order to access our systems, it may be necessary for the IT Department to install software applications on your device. If you remove any such software, your access to our systems will be disabled.

4.4. The School reserves the right, at any time, for any reason and without prior notice, to (temporarily or permanently) disconnect, disable, restrict use of or modify access to the School's systems via a device.

5. Security requirements

5.1. You must comply with our ICT Usage Including Photograph and Mobile Phone policy for all staff which is available from the X drive when using a device to connect to our systems.

5.2. In addition, you must ensure that you:

(i)

5.2.1. do not leave a device logged in and unattended - you must always lock the device when leaving it unattended;

5.2.2. do not allow a device to be accessed by others when you are present and logged in; and

5.2.3. disconnect from the School's systems when you have finished work.

5.3 Work devices are configured to standard security and other settings before being issued to staff. These settings must not be changed. If any changes are required to these settings, approval must be sought from the IT Department.

5.4 **Security requirements for personal devices**

5.4.1 In addition, and to the extent our ICT Usage Including Photograph and Mobile Phone policy for all staff does not address the issues below, you must:

5.4.1.1 at all times, use your best efforts to physically secure the device against loss, theft or use by persons who we have not authorised to use the device. You must secure the device whether or not it is in use and whether or not it is being carried by you. This includes, but is not limited to, passwords, encryption, and physical control of the device;

5.4.1.2 install any anti-virus or anti-malware software at our request before connecting to our systems and consent to our efforts to manage the device and secure its data, including providing us with any necessary passwords;

5.4.1.3 [comply with our device configuration requirements;]

5.4.1.4 protect the device with a unique PIN number or strong password not used for any other purpose, and keep that PIN number or password secure at all times. The PIN number or password should be changed regularly. If the confidentiality of a PIN number or password is

(i)

compromised, you must change it immediately. The use of PIN numbers and passwords should not create an expectation of privacy by you in the device;

5.4.1.5 maintain the device's original operating system and keep it current with security patches and updates. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing our systems or school data;

5.4.1.6 prohibit use of the School's systems by anyone not authorised by us;

5.4.1.7 not download or transfer any school data to the device, for example via e-mail attachments, unless specifically authorised to do so. Staff must immediately erase any such information that is inadvertently downloaded to the device;

5.4.1.8 not install apps from untrusted or unverified market-places;

5.4.1.9 not backup the device locally or to cloud-based storage or services where that might result in the backup or storage of school data. Any such backups inadvertently created must be deleted immediately; and

5.4.1.10 not use the device as a mobile hot-spot or use public unsecured Wi-Fi to access our systems without our prior consent.

5.4.2 We reserve the right to inspect your device and access data and applications on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the school data on it for legitimate business purposes, which include (without limitation) enabling us to:

5.4.2.1 inspect the device for use of unauthorised applications or software;

(i)

5.4.2.2 inspect any school data stored on the device or on backup or cloud-based storage applications and prevent misuse of the device and protect school data;

5.4.2.3 investigate or resolve any security incident or unauthorised use of our systems;

5.4.2.4 conduct any relevant compliance obligations (including in relation to concerns regarding confidentiality, data protection or privacy); and

5.4.2.5 ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy).

5.4.3 You must co-operate with us to enable such inspection, access and review, including providing any passwords or PIN numbers necessary to access the device or relevant applications. A failure to co-operate with us in this way may result in disciplinary action being taken against employees (up to and including dismissal) and, in the case of a breach of this policy by a casual or agency worker, the termination of the engagement.

5.4.4 If we discover or reasonably suspect that there has been a breach of this policy, including any of the security requirements listed above, we shall immediately remove access to our systems and, where appropriate, remove any school data from the device. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from school data in all circumstances. You should therefore regularly backup any personal data contained on the device.

5.4.5 By signing the declaration at the end of this policy, you understand that it may be necessary and lawful for us to, without further notice or permission, inspect a device and applications used on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the data on or from a device for the legitimate business purposes set out above.

(i)

5.4.6 We will not track any personal devices via GPS or location based Wi-Fi without your or the device owner's permission.

6 Lost or stolen devices

6.1 In the event of a lost or stolen device, or where a staff member believes that a device may have been accessed by an unauthorised person or otherwise compromised, the staff member must report the incident to the IT Department and Deputy Head immediately.

6.2 Appropriate steps will be taken to ensure that school data on, or accessible from, the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all school data on the device (including information contained in a work e-mail account, even if such e-mails are personal in nature). Although we do not intend to wipe other data that is strictly personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from school data in all circumstances. You should therefore regularly backup all personal data stored on the device.

7 Data security breach

If you become aware of a breach of security, or believe that a device may have been accessed by an unauthorised person or otherwise compromised, you must inform the IT Department and Deputy Head as soon as possible and in any event by no later than close of business on the relevant day. Further details on data security breaches can be found in the School's ICT Usage Including Photograph and Mobile Phone policy for all staff.

8 Personal data

8.1 The School has a lawful basis on which to access and protect school data stored or processed on a device (whether owned personally or by the School), including the content of any communications sent or received from the device. However, we recognise the need

(i)

to balance our obligation to process data for legitimate purposes with your expectations of privacy in respect of your personal data. Therefore, when taking (or considering taking) action to access your device or delete data on your device (remotely or otherwise) in accordance with this policy, we will, where practicable:

8.1.1 consider whether the action is proportionate in light of the potential damage to the School, staff, parents, pupils or other people impacted by school data;

8.1.2 consider if there is an alternative method of dealing with the potential risks to the School's interests or the interests of others (recognising that such decisions often require urgent action);

8.1.3 take reasonable steps to minimise loss of, and access to, your personal data, although we shall not be responsible for any such loss or access that may occur; and

8.1.4 delete any such personal data that has been copied as soon as it comes to our attention (provided it is not personal data which is also school data, including all personal emails sent or received using our email system).

8.2 To reduce the likelihood of the School needing to access your personal data, or the personal data of third parties, held for non-work related purposes, you must comply with the following steps to separate school data from your personal data on the device:

8.2.1 organise files within the device specifically into designated folders that clearly distinguish between school data and personal data (for example, marking your own folders as "PERSONAL");

8.2.2 do not use work e-mail for personal purposes, but if you do ensure that it is labelled appropriately in the subject line; and

8.2.3 regularly backup all personal data stored on the device.

9 Monitoring

9.1 The contents of our systems and school data are our property. All materials, data, communications and information, including but not limited to e-mail (both outgoing and

(i)

incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device (collectively referred to as **content** in this policy) during the course of business or on our behalf is the School's property, regardless of who owns the device.

9.2 We reserve the right to monitor, intercept, review and erase, without further notice, all content on the device that has been created for the School or on its behalf. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the device as well as keystroke capturing and other network monitoring technologies, whether or not the device is in your possession.

9.3 It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore you should have no expectation of privacy in any data on the device. Staff are advised not to use our systems for any matter intended to be kept private or confidential. If you use a device to process personal data about third parties (for example your family and friends) for personal purposes you should be aware that this may be inadvertently monitored, intercepted, reviewed or erased. You should ensure that any third parties are aware that their personal data may be inadvertently monitored.

9.4 Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law and the School will follow relevant School policies, including the Privacy Notice, when doing so. It will take place in order for the School to comply with a legal obligation or for our legitimate school purposes, including, without limitation, in order to:

9.4.1 prevent misuse of the device and protect school data;

9.4.2 ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy);

9.4.3 monitor performance at work;

(i)

9.4.4 ensure that staff members do not use our facilities or systems for any unlawful or inappropriate purposes or activities including those which may risk the safety or wellbeing of pupils, parents or other members of staff; and

9.4.5 protect the School's reputation.

9.5 We may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. We may obtain and disclose copies of such content or of the entire device (including personal content) for disciplinary investigations.

9.6 By signing the declaration at the end of this policy, you acknowledge that St Hilary's is entitled to conduct such monitoring where it has a legitimate basis to do so, and you confirm your agreement (without further notice or permission) to our right to copy, erase or remotely wipe the entire device (including any personal data stored on the device). You also agree that you use the device at your own risk and that we will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.

10 Technical support

The School will provide technical support for work devices and, where possible, it will provide technical support for personal devices. For the avoidance of doubt, the School cannot support private or third party broadband connections to the internet and is not responsible for their speed or availability.

11 Costs and reimbursements

11.1 For work devices, the School will cover the costs associated with use for work purposes (excluding any fees incurred and for the adherence to the terms and conditions of your broadband service, including download limits). For more information on device reimbursement procedures, please read our Staff Handbook or contact the Business Manager.

(i)

12 Staff departure

12.1. On your last day of work (regardless of the reason for your departure):

12.1.1 your access to the School's systems and applications will cease;

12.1.2 in respect of work devices, your device must be returned to the School; and

12.1.3 in respect of personal devices, all school data (including work e-mails), and any software applications provided by us for work purposes must be permanently removed from the device.

12.2 For the avoidance of doubt, if a personal device is repaired, exchanged, sold, given away or otherwise disposed of, the provisions within paragraph 12.1.3 must be complied with.

Reviewed: April 2020
Next review date: April 2020
Person responsible: Gemma Mitchell

DECLARATION AND AGREEMENT

I explicitly confirm my understanding and agreement to the following:

- I have read, understood and agree to all of the terms contained in the Remote Working: Mobile Device Policy.
- I understand that the terms of this policy will apply to me at all times when working remotely, either during or outside office hours.
- I acknowledge and agree that authorised personnel of the School shall have the rights set out in this policy, including but not limited to the right to access, monitor, review, record and wipe (as the case may be) data contained on a device (including a personal device) which I acknowledge may result in inadvertent or necessary access to or destruction of my personal data.
- I understand and agree that the School at its discretion may amend (or remove) this policy at any time and that I will be bound by the terms of the policy as amended.

……

SIGNED

……

FULL NAME (in capitals)

……

DATE

Please return the completed form to the Deputy Head.