GENEVA ENGLISH SCHOOL

REMOTE WORKING & USE OF PERSONAL DEVICES POLICY

INTRODUCTION

To enable GES to maximise its employees' effectiveness and productivity, the School is committed to supporting 'remote working'. GES aims to provide the environment and tools to reap the benefits of adopting flexible working practices to meet the needs of the School, its staff and the pupils.

Portable computing devices are provided to assist certain members of staff to conduct official school business efficiently and effectively. This equipment and any information stored on it should be recognized as valuable organisational information assets and safeguarded appropriately.

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 school IT equipment and personal IT equipment when working onsite and away from the school's premises (ie working remotely).

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 Switzerland.

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

- Desktop computers
- Laptop computers
- Tablet computers
- Mobile phones including smartphones
- Smart watches

USE OF THE SCHOOL'S IT SYSTEMS AND DEVICES

The School's IT systems and any school-owned digital device issued to members of staff are intended for school purposes only. All IT equipment supplied to users remains at all times the property of Geneva English School. Equipment must be returned at the request of GES.

TELEPHONES

Where appropriate, the School may provide access to a telephone system for remote working. It is recommended that calls made for school purposes should be carried out using the telephone systems in school. If the employee uses their own telephone line, or mobile phone including smart phones, charges for business calls (excluding line rental) will not be reimbursed.

OTHER EXPENSES

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

WORKING REMOTELY

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

Sensitive material or personal data must be disposed of by recognised methods using office based shredding equipment or other means. Further guidance on this can be found in the school's Data Protection Policy.

Members of staff must ensure that:

- Any confidential data that is transported from one location to another is protected by encryption or pseudonymised and that school data security protocols are followed when using any such data at any location. Laptops or other portable equipment must never be left unattended in cars or taken into vulnerable areas.
- School IT systems are only accessed using their own username and password and that school usernames or passwords are not shared with anyone else. When signing into school-based systems, passwords should not be saved on the device and only work-related documents should be downloaded to a school device.
- They enable the 'Filevault' encryption tool on any school-owned Macbook for which they have responsibility, following the instructions provided by the Head of Computing.
- Where a wired connection is not possible and a wireless connection is used, it is a secure connection.
- No other family members use school-owned equipment. The school-owned equipment is supplied solely for the staff member's use.
- They do not use IT equipment for school purposes where it can be overlooked by unauthorised persons and do not leave it unattended in public places.

The School may at any time, and without notice, request a software and hardware audit and may require the removal of equipment at the time of the audit for further inspection. All users must cooperate fully with any such audit.

Paper documents must be stored in a lockable cupboard and kept out of sight of anyone except authorised employees of GES. Paper documents that are no longer needed should be destroyed in line with our Data Retention Policy.

Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should be located out of sight of the casual visitor. School-owned equipment must be kept safe and secure whenever it is not in use.

ACCESS CONTROLS

It is essential that access to all school information is controlled. This can be done through physical controls, such as locking the school office, home office, classroom or locking the

computer's keyboard. Alternatively, or in addition, this can be done logically such as by password or user login controls.

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 school data held on the portable device must be encrypted.

GES may at any point use Information Rights Management for sensitive data. This prevents any user from printing or forwarding sensitive pieces of information that the school feels requires extra protection.

As compliance criteria imposed on the School become more complex, the Head of Computing may need to apply further security controls from time to time. Any such changes will be communicated to all staff with access to a school computer. Such security controls may be applicable to school owned and personal devices. Should the user not wish their privately owned device to be subject to security controls then that device may not be allowed to connect to the school network or access school information.

USE OF PERSONAL DEVICES

Members of staff are permitted to bring in personal devices for their own use. They should be mindful that pupils are not allowed to use personal devices in school without permission and should therefore use their own mobile phone in a way that is discreet and respectful to the pupils. Where possible, use of a mobile phone by staff should take place in staff areas, away from the children. Such use should be for legitimate reasons and should not interfere with a member of staff's productivity or official school duties.

Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the Head of Computing.

Where permission is given for use of personal devices for school purposes, they must be password protected. They must not be left unlocked when unattended and must have up to date antivirus software and security updates installed. Staff should be cautious about the security of their personal device i.e. whether or not their smartphone has been 'jailbroken' or 'rooted' and whether the device can be configured with 'auto-wipe'.

The Head of Computing will help staff connect their device to the School's wireless network and access school systems such as the School Database (School Manager), storage platforms (Google Drive) and e-mail (Gmail) but cannot provide support for the device.

All official school business must be conducted on the School's IT systems, and personal email accounts should not be used for school business. Limited, occasional use of electronic media (sending or receiving) or the Internet for personal purposes is understandable and acceptable. Such use must not adversely affect the systems' or devices use for educational purposes. Members of staff are expected to demonstrate a sense of responsibility and not to abuse this privilege.

School documents should be saved to user's GES Google Drive account and not on personal devices for any reason. GES-related photographs should be saved to the GES Cloud, which should only be accessed onsite.

When using the Internet on personal devices in school, staff must never distribute malicious software, to damage, interfere with, or gain unauthorized access to the computer systems of others, or carry out illegal activities.

Staff must not download any software or resources from the Internet on personal devices that could compromise the network, or are not adequately licensed. Any school software requirements should be discussed with the Head of Computing, who will authorise the software installation.

PHOTOGRAPHY

The use of a personal mobile phone to take pictures of pupils (or that contain images of pupils incidentally) either in or out of school is prohibited. This is to protect members of staff from allegations of inappropriate behaviour.

If a personal phone is used inadvertently in this way, any images must be uploaded to the GES Cloud at the earliest opportunity and deleted from the personal device with no copies having been kept or transmitted elsewhere. The School may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy.

When taking images of pupils (or that contain images of pupils) in school or on school trips I will always use school-owned cameras or iPads and comply with the School's policy on Taking, Storing and Using Images of Children, which is published on the School's website.

MONITORING

Staff should be aware that use of the School's e-mail and internet can be monitored. Both web history and school email accounts may be accessed by the School where necessary for a lawful purpose, including the investigation of serious misconduct, welfare concerns, concerns about extremism and for the protection of others.

Connecting a personal digital device to the School's wifi network will result in the School's monitoring:

- The name of the device;
- The date and time the device was last used on the network;
- The IP address of the device.

All school-owned devices are added to the School's Management Device Monitoring (MDM) software and in the event a school device is lost, data will be wiped from the device remotely to prevent a data breach. This includes any school files, calendar events or e-mails that are linked to a personal device. The loss of any school-owned or personal device containing school data must be reported immediately to the Head of Computing.

IT SUPPORT AND MAINTENANCE

Members of staff are responsible for any repairs or technical support required for their own personal devices. School equipment will be repaired by the Head of Computing or by the School's external IT consultants.

All school IT equipment is covered under the manufacturer's limited warranty. Insurance is in place to cover accidental loss or damage. If school-owned equipment is lost, damaged, or stolen, the member of staff responsible for that equipment must immediately report this to the Head of Computing and describe the circumstances surrounding the loss, damage, or theft of the device.

In the event of the hardware or software failure of a school device, members of staff must bring it to the Head of Computing, who will assess the issue and if necessary use the services of our external consultants (ART Computer).

Members of staff are liable for the cost of damages to school IT equipment caused by:

- improper use, abuse, neglect, and alterations;
- improper service, improper installation, and improper connections with other peripheral devices (for example linking to printers or servers that are not school approved equipment);
- loss or misplacement that is not accidental.

BREACHES OF THIS POLICY AND CONCERNS ABOUT ONLINE BEHAVIOUR

The School reserves the right, at its discretion, to review any employee's school-owned electronic device to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other school policies, to assist in the investigation of wrongful acts, or to comply with any legal obligations of the School in its role as employer or generally. Deliberate breaches of this policy will be dealt with as a disciplinary matter using the School's usual procedures.

Author: Ronan McStravick, Head of Computing & Digital Strategy and e-Safety Officer
Created: September 2018
Review date: July 2019