AVON HOUSE
PREPARATORY SCHOOL

CELEBRATING & SUPPORTING EVERY CHILD

Staff Policy on Mobile Phone, Technology, Security and Electronic Communications

Introduction

Technology has advanced significantly over the last few years - and it continues to evolve. Wireless connections in particular have extended the capabilities of mobile phones, enabling access to a wide range of new content and services globally. Many phones now offer Internet and email access, alongside the most often standard functions of messaging, camera, video and sound recording. Mobile phones, alongside other forms of technology are changing the way and speed in which we communicate. They can provide security and reassurance; however there are also associated risks. The introduction of wearable technology has also become a factor. As with e-safety issues generally, risks to children and young people can be broadly categorised under the headings of content, contact and conduct and managed by reducing availability, restricting access and increasing resilience.

Aim

The aim of this policy is to promote safe and appropriate practice through establishing clear and robust acceptable use guidelines.

This is achieved through balancing protection against potential misuse with the recognition that mobile phones are effective communication tools - which in turn can contribute to safeguarding practice and protection.

Scope

The policy covers all staff and provides guidelines on work equipment and personal equipment, where these are used for work purposes. This policy must be read in conjunction with the School's staff handbook, the School's Social Media and Networking Sites Policy, Data Protection Policy, and Privacy Notice. The policy covers

- the internet and servers
- all forms of electronic communication – email, social media etc.
- electronic bulletin boards and social media
- file sharing by whatever means
- computing devices including desktops, laptops, printers, mobile devices, etc.
- communications equipment including telephones, mobiles, wearables, video conferencing, etc.

Policy statement

It is recognised that it is the enhanced functions of many mobile phones that cause the most concern, and which are most susceptible to misuse. Misuse includes the taking and distribution of indecent images, exploitation and bullying.

It is also recognised that mobile phones can cause an unnecessary distraction during the working day and can be intrusive when used in the company of others.

When mobiles phones are misused it can impact on an individual's dignity, privacy and right to confidentiality. Such concerns are not exclusive to children and young people; hence there is a duty to protect the needs and vulnerabilities of all.

It is appreciated that it can be very difficult to detect when such devices are present or being used, particularly in relation to enhanced functions, such as cameras. The use of all mobile phones is therefore limited, regardless of their capabilities. The aim is to avoid distraction and disruption of the working day, and to minimise the opportunities for any individual to make any covert images or misuse functions in any other way.

Staff mobiles must be switched off and out of sight during the school day including extra curricular clubs. If a member of staff wishes to use their mobile phone they must go to the staff room, school reception or off-site.

A zero-tolerance policy is in place with regards to the use of personal or work-related mobiles by any individual in classrooms and playground. Mobile phones must be placed in the tin provided when in class. Specialist staff and midday supervisors should put their phones in the tin provided in the school office.

Confidential Information

Employees must not access or attempt to access confidential data unless they are authorised to do so. Confidential information should only be used for its intended purpose. The following is prohibited

- Using confidential information for anything other than its intended use
- Use of School's proprietary information for personal use
- Leaving your computer unattended with confidential files logged on to your system
- Leaving computer disks unattended in easy to access places with confidential data
- Sending confidential information over the internet on unsecured communication lines without prior approval

General Rules and Monitoring

The School reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law and the School's policies and procedures.

Employees should not assume electronic communications are totally private. Accordingly, if they have particularly sensitive information to transmit, they should use other means.

The following must be adhered to:

- Employees must regularly back up essential files and store back-ups securely.
- Employees handling personal data and sensitive personal data must ensure compliance of data protection regulations.
- Employees are required to turn off their computer and screen at the end of the day and when not in use for an extended period of time.
- When printing to a printer in an unsecured area ensure documents are picked up in a timely manner.
- If you observe a document at a shared printer, or any other location, do not read it without permission.
- Position the computer monitor in a way that confidential information cannot be viewed by unauthorized people.
- Respect the intellectual property of the School, its clients and third parties and follow good practice at all times.
- Connections (either through the School's laptop or mobile phone) to public or open networks is not allowed as this may be used as an entry point for hackers. When no other safer alternative is available, employee must log out of School systems and remote connections to the School network before using such network.
- Do not open attachments or URL links unless they are from a trusted source. If in doubt, verify authenticity by calling or emailing the sender.
- Comply with the Staff Use of Social Media and Networking Sites policy when using social media for business purposes and when using the name of the School in a social forum.
- Do not share sensitive School information or client information when using social media either for business or personal purposes.
- Use of School email addresses for non-business purposes (including registration on non-business related websites) is strongly discouraged.
- Personal email accounts must not be used to conduct School business.
- Use of email manipulation techniques to disguise identities or to generate unsolicited emails is prohibited.
- Electronic devices must not be used to send or receive discriminatory, threatening, derogatory or pornographic communication.
- Unauthorized copying, redistributing, and republishing of copyrighted or proprietary material are strictly prohibited.
- Do not install any additional software program without prior approval from your manager / IT department.
- Passwords of any nature are not to be shared with colleagues.

Devices and Technology
Personal use of work equipment

Electronic media and services are provided by the School for business use. Limited, occasional, or incidental use (sending or receiving) for personal, non-business purposes is

understandable and acceptable. All such use should be done in a manner that does not negatively affect the use of the School's systems for business purposes. Employees are expected to demonstrate a sense of responsibility and not abuse this privilege. Personal use must not

- interfere with work
- adversely affect IT security
- create a significant overload on the School's technology

Any personal data owned on a School work equipment must be segregated from work related data to ensure privacy and must be saved within a single clearly named folder.

Physical Protection of School Equipment

Employees must

- physically securely store unattended School provided devices out of sight at home and outside.
- activate screen lock on their devices
- report immediately if any of the devices gets stolen or lost so appropriate steps can be taken to minimise leakage or loss of School held information.

Employee Duties

Employees who are issued with School equipment such as a mobile phone are responsible for the security of the phone and should take all reasonable steps to ensure its safekeeping. All employees with a mobile phone are required to use a PIN code and to keep this confidential. This is especially important if you have a Smartphone, as this can provide access to our email system.

Employees issued with School equipment agree that they will be responsible for ensuring they are properly looked after and stored safely at all times. Employees will be required to pay to the School the reasonable replacement cost of any item of office equipment, which is lost or stolen whilst under their control due to their negligence or deliberate or reckless act or omission. Employees further agree to provide their written consent for the School to deduct a sum equal to the reasonable replacement cost from their wages should an item of office equipment be lost or stolen whilst under their control due to negligence or deliberate or reckless act or omission.

The School reserves the right to require employees to return any item of office equipment at any time during their employment for any reason whatsoever, including, but not limited to, the withdrawal of any privilege of working from home and/or working away from the School's premises. Employees have no contractual entitlement to the use of the office equipment and therefore withdrawal of its use at any time does not entitle you to claim any form of damages or compensation.

In addition, on the termination of employment for any reason, employees are expected to promptly and without unreasonable delay return any items of office equipment and, in any event, this must take place by no later than any date specified to you at the time by the School. Any items of office equipment must be returned in the same condition as provided, subject to reasonable wear and tear.

Use of Passwords and School provided credentials

Employees must

- use unique passwords and PIN
- not share with anyone other than to their line manager or to the relevant IT professional
- change passwords routinely and at any indication of a system compromise

Personal mobiles

Effective guidance is in place to avoid the misuse of mobile phones causing unnecessary disruptions and distractions at school, and to ensure effective safeguarding practice is promoted to protect against potential misuse.

Staff are not permitted to have their mobile phones on during school hours and there is a clear expectation that if they need to use their mobile they will go off-site or go to the staff room or school reception to do so.

Other than in agreed exceptional circumstances, phones must be switched off and calls and texts must not be taken or made during the school day outside of the designated times.

Staff are not permitted, in any circumstance to use their phones for taking, recording or sharing images and 'mobile free' areas must be observed at all times unless consent has been sought from the Head Teacher, for example whole school outing where there are not enough school devices.
Staff are not permitted to use their own personal phones for contacting pupils and their families within or outside of the setting unless by prior arrangement with the Head Teacher.

Parents, visitors and contractors are respectfully requested not to use their mobile phones in any of the designated mobile free areas. Should phone calls and/or texts need to be taken or made, use is restricted to those areas not accessed by pupils in order to avoid any unnecessary disturbance or disruption to others.

Under no circumstances is any individual permitted to take images or make recordings on a mobile phone without the Head Teacher's consent.

Any individual bringing a personal device into the setting must ensure that it contains no inappropriate or illegal content.

Home working

Employees who work regularly from home must follow the School's computer security protocol. School equipment must not be used by other members of the family as this may lead to a breach of security. Employees must ensure that the equipment is password protected and is kept in a secure place when not in use.

Driving

If any practitioner is required to drive in a working capacity, and has responsibility for the work mobile, the phone must be switched off whilst driving. It is strongly recommend that practitioners follow the same procedures regarding their own personal mobile phones.

Under no circumstances should practitioners drive whilst taking a phone call. This also applies to hands free and wireless connections, which are considered a distraction rather than a safer alternative.

Policy for pupils

The school policy is that pupils should not bring mobile phones or any form of electronic communication devices to school except in mitigating circumstances. If a parent has asked specifically for their child to be allowed a mobile phone as they are walking home alone (or a similar situation) then the child will give the phone to their class teacher who will keep it in a safe place until the end of the school day.

If a pupil is found in possession of a mobile phone (not in the above circumstances) it will be confiscated by a member of staff for the remainder of the school day. The member of staff will keep the mobile phone in a safe place until the end of the school day when it will be returned to the pupil. If this happens more than once the mobile will be returned to the parent or carer so that the school can explain why mobile phones are not permitted.

Policy violations

Any violations or suspected violations must be reported immediately. Any non-compliance with the above policy will be dealt with through the School's disciplinary policy.

This policy will be reviewed by the Senior Leadership Team on a regular basis.

Reviewed June 2016 AC
Reviewed August 2018 SFBC/AC
Reviewed May 2019 AC
Reviewed August 2020 AC