THE OUTDOORS GROUP

The Outdoors School

THE OUTDOORS SCHOOL SOCIAL MEDIA AND IT POLICY

Company number: 10755829

Introduction

The IT infrastructure is owned by the school and is made available to learners to further their education and to staff to enhance their professional activities including teaching, research, administration and management. This policy has been drawn up to protect all parties – the learners, the staff and the school.

If a member of staff breaches this policy, then disciplinary action may be taken.

Protocol for use of The Outdoors School owned Mobile Technology Devices.

Users of The Outdoors School mobile technology devices are responsible for the following:

- Ensuring the device is protected by a password or pin code
- Returning the device to the School Office when it is no longer required
- Only using official stores for installing apps e.g. Microsoft store, Apple store, Google Play
- Not changing security settings or amending configuration files. This includes disabling passwords, pin codes and any installed security programs (e.g. Anti- Virus software)
- Notifying the Business Services Team in the event that the device is lost or stolen
- When using your school device:
    - Turn it off and put it in an appropriate carrying case when travelling
    - Take care when connecting the network cable and seating the device on a docking station as the connections can be easily damaged
    - Keep all drinks and any other liquids away from your device. Any spillage can result in data loss and expensive repairs
    - Do not leave the device in full view in a vehicle, even for a short period of time. It must be locked in the boot when the vehicle is left unattended and not left in the vehicle overnight
    - Lock it away in a drawer or cupboard if left unattended on site for an extended period of time or over-night
    - Never leave it unattended in public places
    - If travelling by air, devices must always be carried in the cabin and never checked in to the hold
    - Staff must not use these devices in certain areas within the school site, e.g. changing areas and toilets
- Only take photographs/still images or video footage of learners using school equipment, for purposes authorised by the school. Any such use should always be transparent and only occur where parental consent has been given. The resultant files from such recording or taking of photographs must be stored in accordance with the schools' procedures.
- Staff who leave The Outdoors School must return all school devises immediately.

Installation of Software:

- Staff must make a request to the Business Services Team for the installation of academic or administrative software on any device or for learners to access. This includes upgrades to packages already installed.
- Software will only be installed on the school's devises if there are the appropriate licences, and if its use is in accordance with its licensing rules

- Unless explicitly authorised, all school's software is for teaching and learning use, or for the purposes of the school's business and administration
- Staff and learners who leave The Outdoors School must remove all school software and data immediately from any personal devises.

Protocol for use of Personal Mobile Technology Devices
The purpose of this protocol is to prevent unacceptable use of mobile phones, camera-phones and other handheld devices by the school community, and thereby protect the school's staff and learners from undesirable materials, filming, intimidation or harassment.

Should these devices be misused, there will be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to learners, so the needs and vulnerabilities of all must be respected and protected.

It is to be recognised that it is the enhanced functions of many devices that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse include the taking and distribution of indecent images, exploitation and bullying.

Staff are to be aware of the following:
- The school reserves the right to search the content of any device on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Personal devices brought into school are the responsibility of the device owner. The company accepts no responsibility for the loss, theft or damage of these items.

Staff must:
- not use personal devices to take photos or videos of learners. They should only use school owned equipment for this purpose
- not use these devices in certain areas within the school site, e.g. changing rooms and toilets
- not use their own devices for contacting learners or their families within or outside of the setting in a professional capacity. Staff will be provided with a school device where contact with learners, parents or carers is required
- switch off personal devices or switch to 'silent' mode during the school day. Bluetooth communication should be 'hidden' or switched off and must not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- in an emergency where a staff member doesn't have immediate access to a school owned device, they should use their own and hide their mobile number (by inputting 141) for confidentiality purposes.

Learners can:
- use their own devices for specific learning activities under the supervision of a member of staff
- have a device for their own safety, where this has been requested by the parent (this will however need to be handed in at the start of the day and returned at the end of the day unless being used for a specific learning activity)

- have their device confiscated if this policy is not adhered to. The device will be held in a secure place in the school office and released to parents or carers in accordance with the school policy
- not take devices into examinations. Learners found in possession of a personal device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- contact their parents or carers, using a school device, if the need arises. Parents and carers are advised not to contact their children directly during the school day, but to contact the school office
- and should, protect their contact details by only giving them to trusted friends and family members. Learners will be instructed via curriculum time in safe and appropriate use of mobile technology devices and will be made aware of boundaries and consequences.

Digital Communication

The following good practice must be followed:

- Any digital or written communication between staff and learners or parents/carers must be professional in tone and content
- Any digital or written communication may be monitored and may be subject to a subject access request, therefore no digital or written communication can be considered private and confidential, therefore must always be written with this knowledge
- Any emails that are received which make a user uncomfortable and/or are threatening or bullying in nature should be reported to the line manager or designated safeguarding lead. Staff should not respond to these communications.
- Learners are only contacted via school authorised mechanisms. At no time should personal telephone numbers, email addresses or communication via personal accounts on social media platforms be used to communicate with learners
- Parents and carers are only contacted using school telephone numbers, email addresses and social networking sites that are set up for professional purposes and approved by the school. It is prohibited for staff to use their personal devices or personal accounts on social media platforms to contact parents and carers.

E-Safety and Internet Use

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The use of these exciting and innovative tools in school and at home have been shown to raise educational standards and promote learner achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss or sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing or distribution of personal images without an individual's consent or knowledge
- Inappropriate communication or contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video or internet games

- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision, to build learners' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.
Staff must:

- not access pornography; neither should personal equipment containing pornographic images or links to them be brought into school
- not engage in inappropriate use of social network sites which may bring themselves, the school, school community or The Outdoors Group into disrepute
- exercise caution in their use of all social media or any other web-based presence they may have, including written content, videos or photographs, and views expressed either directly or by 'liking' certain pages or posts established by others. This may also include the use of dating websites where staff could encounter students either with their own profile or acting covertly
- not link themselves with the school on any social network site they use unless with prior consent of the Senior Leadership Team
- not respond to negative comments posted online but bring this to the attention of the Senior Leadership Team
- must report to the Senior Leadership Team any inappropriate contact by a learner or their family

In summary staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and the relevant school and company policies
- they report any suspected misuse or problem to the Senior Leadership Team for investigation and action
- digital communications with learners are on a professional level and only carried out using official school systems
- they monitor technology use in lessons and school activities
- they are aware of e-safety issues related to the use of mobile technology devices and that they monitor their use and implement school policies with regard to these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Responding to Incidents of Misuse
Any apparent or actual misuse which appears to involve illegal activity, will be reported to the Senior Leadership Team and the Designated Safeguarding Lead, examples include:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material

- other criminal conduct, activity or materials

Actions will be followed in line with the school procedures, including reporting the incident to the police and the preservation of such evidence. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. Such incidents of misuse will be dealt with through the normal behaviour management policy.

Following Copyright Laws

The Copyright laws of the UK and other countries must not be infringed. Downloading material from the internet carries the risk of infringing copyright. This applies to files, music, films, TV programmes, documents and software, which must be licensed. Material illegally copied in this country or elsewhere and then transmitted to another country via the internet, will also infringe the copyright laws of the country receiving it. Any uploading or downloading of information through on-line technologies which is not authorised by the copyright owner will be deemed to be an infringement of her/his rights. Users must not make, transmit or store an electronic copy of copyright material.

Date issued/reviewed/amended: 11th June 2020

Signature of Director or Company Secretary:

Name: Shevek Pring

Review date set: 1st June 2021

This policy in all its forms and copies are the property of The Outdoors Group Ltd. The Outdoors Group Ltd accepts no responsibility for misinformation caused by unauthorised copying, distribution or amending of policy documents where they exist in the public domain.

Company number: 10755829