Acceptable use of IT Equipment Policy

Policy Lead:	**Assistant Head - EA**
Last Review Date:	September 2021
Next Review Date:	September 2022
Approval needed by:	**Headteacher**

THE LEARNING ALLIANCE

1. Acceptable Use of IT Equipment

1.1 The Oaks Academy provides its staff with IT equipment for the purpose of carrying out their role. Staff must respect that this equipment does not belong to them and ensure that they care for it appropriately. Equipment includes, but is not limited to: PCs, laptops, tablets, mobile phones, scanners, photocopiers, hand-held devices and removable media etc.

2. General Care of Equipment

2.1 Staff must:

a) keep equipment in good order, i.e. take care not to drop the equipment or put in it harms way (trail wires across offices, leave it on the floor etc).
b) secure equipment when leaving it, even for a brief period.
c) take all reasonable steps to keep equipment secure both in the workplace and outside of the workplace, including whilst transporting equipment.
d) respect the confidentiality, integrity and security of software and data which they may have access to.
e) comply with the terms of any licence agreement between the school and a third party governing the access to software or data; and
f) report any lost or stolen devices to the headteacher IMMEDIATLEY

2.2 When using School equipment staff must NOT:

a) permit access to equipment or disclose any username and passwords to any other person including friends, family, or colleagues.
b) share usernames or passwords with any individual or write passwords down.
c) impersonate any other staff member when using equipment or systems.
d) Install unauthorised software.
e) copy, modify, delete, disseminate, or use software without appropriate permission.
f) deface or personalise equipment (as it will be reused).
g) purchase or dispose of any work equipment themselves, they must contact the headteacher to approve the purchase new equipment or the IT service desk to arrange disposal of the equipment; and
h) access, attempt to access, circumvent, attempt to circumvent, established security mechanisms or controls, to view, modify, delete, or transmit information and/or information systems to which they have not been given explicit access or authorisation

Key Point: Never share your password or log-in details with anyone. If anyone else asks to use your password remember that it is against the school's policy and could lead to disciplinary action. If you receive a call or email asking for your password, you must refuse - the IT department will never ask you for your password.

3. Keeping IT Equipment Secure:

3.1 Staff must:

a) always lock their computer (using the Ctrl-Alt-Del sequence) or log off when leaving it for any significant period.
b) take care to avoid being overlooked when using the computer in a public place, do not sit with the screen facing a window where members of the public pass by.
c) never email personal or confidential information to their home email address so that they can work on the information later.
d) When transporting IT Equipment staff must:
(i) use a suitable bag to transport any equipment.
(ii) never write down login details or passwords and must never write this information down and keep in with the equipment, or in handbags, coats etc.
(iii) never leave laptops or any other mobile computing devices in plain sight when travelling. If travelling by car, all devices must be locked in the boot. Staff must never leave any mobile computing device in a car overnight.
(iv) (When travelling on public transport) always keep the laptop/bag near and thus minimise the risk of theft.
(v) never leave equipment unattended in luggage bays or overhead racks; and
(vi) whilst travelling on public transport ensure that your screen cannot be viewed/read by unauthorised persons. Overlooking (shoulder surfing) and eavesdropping are the greatest risks when working remotely in public locations such as trains, hotel public areas and coffee shops.

4. Downloading Applications onto Corporate Devices

4.1 Staff are permitted to install applications for personal use if they are used reasonably; for example, using the BBC News App during lunch is acceptable but using eBay during work time is not.

4.2 Staff must NOT:

a) use applications which are not for Corporate Use during work time except for radio or music applications. Music or radio applications can be used subject to manager's discretion; however, staff must not stream music or radio as this will use excessive data/internet bandwidth.
b) use Apps or download any files that contain indecent, obscene, pornographic, or other offensive materials, sponsor terrorism or other illegal activities.
c) make or post indecent, obscene, pornographic, or otherwise offensive, racist or harassing remarks or materials,
d) use file sharing/storage Apps such as Dropbox or other "Cloud" based solutions other than their Corporate OneDrive account.
e) use the School's Internet connection to play online gaming, in particular staff must not use any site which could be viewed to involve gambling.

f) upload, download, or otherwise transmit any item which may breach its copyright or licence requirements, including the streaming of music or video files; and

g) Facebook, WhatsApp, and other social media apps should be used appropriately and in line with the School's E-Safety and Social Media policies and procedures. Staff must NEVER share personal data over an App unless it is a Corporately approved app (contact the Data Protection Officer or IT department for further details).

5. Keeping Equipment Secure

5.1 Equipment must be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

5.2 Staff must ensure that:

a) equipment is sited to minimise unnecessary access into work areas.

b) screens are suitably positioned, and the viewing angle restricted to reduce the risk of information being viewed by unauthorised persons during their use or a Privacy Screen is used.

c) steps are taken to minimise the risk of potential physical threats, e.g. theft.

d) equipment is reasonably secured from risk of fire, smoke, water (spillages, water leaking through windows), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism (advice on this can be obtained from the IT Team); and

e) staff must avoid eating or drink near to equipment (staff should try and move to another area or a different part of their desk to reduce risk of spillages).

6. Removal of Equipment

6.1 If an individual asks to remove equipment, staff must undertake appropriate checks to ensure the individual has a right to remove the property, i.e. if someone claims to be from the IT service provider, ask them for ID, or contact the IT Department for assurance.

Key Point: Never hand over equipment to a stranger, even if they claim it is an emergency. Incidents have occurred at other organisations where criminals pretending to be IT staff have been given laptops by employees who did not check the person's identity.

7. Acceptable Use of Personal Equipment for Work

7.1 As technology develops more people have high quality IT equipment at home (laptops, desktops, or mobile phones). Staff may wish to use their own equipment for work purposes; this is sometimes referred to as Bring Your Own Device (BYOD). The school permits staff to use their own equipment in line with the following practices:

7.2 Where a personal device is used for work purposes staff must:

a) access the school resources by logging into their School Microsoft Account or connect via Remote Desktop.
b) PIN or Password Protect the device.
c) keep the device secure.
d) regularly update the device to ensure all applications, antivirus and security controls are up to date; and
e) report any lost or stolen devices to the IT Department IMMEDIATLEY so that the school data can be wiped (only the school data will be erased no personal data will be affected).

7.3 Where a personal device is used for work purposes staff must NOT:

a) allow family, friends, children to use the device (unless the access to work areas e.g. emails have been restricted with access controls); and
b) use their personal phone number to make phone calls or disclose their personal phone number to learners or other third parties

7.4 Personal mobiles and electronic devices should not be used for personal use during contact time with children, other than in agreed exceptional circumstances. Own personal phones should not be used for contacting children, young people and their families within or outside school. It is acceptable to use personal devices to contact colleagues for general communication, e.g. to inform your manager that you will be off sick, or late to work.

7.5 Please note: Staff will not be entitled to any form of payment or reimbursement if they choose to use their own device. Any device used is the responsibility of the owner. The school will not be liable to refund the cost of the device, any data usage or other costs associated with using a personal device.