Policy for ICT Equipment -Portable & mobile technology, servers & removable media

Removable Media

- As a user of the school ICT equipment, you are responsible for your activity
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person, ensuring that machines have all appropriate updates including antivirus
- Northern House School logs ICT equipment issued to staff and records serial numbers as part of the school's ICT inventory/Schools' Asset Management. Staff are required to sign for any equipment issued to them in a register. This register is held by ICT support and equipment must be signed in prior to departure.
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made).
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- You are responsible for the backup and restoration of any of your data that is not held on the school's network.
- If there is a requirement for personal or sensitive data to be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device it must be password protected or encrypted.
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to ICT support and signed in. You must also provide details of all your system logons so that they can be disabled
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Policy for ICT Equipment – Portable & mobile technology, Servers & removable media

1 June 2017 Version Number:1

Review Date: Summer Term 2020

Northern House School

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on school systems and hardware can be monitored in accordance with the general policy
- Staff are responsible for ensuring that all school related data is stored on the school network, and not kept solely on the laptop.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. Equipment is not to be taken out of the country unless specifically on school business.
- Synchronise all locally stored data, including diary entries, if relevant, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT Support Team, fully licensed and only carried out by the ICT Support Team
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not wherever possible be left unattended and must be kept out of sight or secured using laptop locks through ICT support if provision required.
- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, tablets, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- Under no circumstances does the school allow a member of staff to contact a student or parent/ carer using their personal device/mobile phone
- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes during school time and it is expected that they are handed in at the gate.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text/picture messages between any member of the school community is not allowed (see Malicious Communications Act an criminal activity linked to the sending or receiving of inappropriate images/messages)
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Servers

- Always keep servers in a locked and secure environment
- Limit access rights to server rooms
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Back-ups are stored in a separate secure location on site
- Data must be backed up regularly
- Backup tapes/discs must be securely stored
- Remote backups should be automatically securely encrypted