Dundee City Council

CHANGING FOR THE FUTURE

Children and Families Service

Use of USB Memory Sticks on the Curriculum Network

The following process applies from **August 2020** for **all** Curriculum Network Users.

Corporate IT Policy states:

'The council discourages the use of USB memory sticks. Employees should avoid their use wherever possible.' *(see over for the full section from the DCC IT policy)*

One Drive

Staff are encouraged to use this secure and easily accessed cloud facility for storage of files, especially those containing personal data. Users have access to the Glow One Drive, and to the DCC One Drive (accessible from the desktop, from mobile devices both personal and school; and from home).

Personal USB Storage Devices (pen drives, hard drives, flash drives, thumb drives, hard drives)

If these have to be used by staff as an exception, they **must be secure** - **suitably encrypted and password protected** *(as is the case in other local authorities e.g. Angus).* Schools are expected to ensure that all staff adhere to this instruction.

Schools can purchase devices through IT procurement, for business use, although privately purchased devices will be allowed if they are secure.

GDPR and AUP

Staff are reminded of their data and network security responsibilities, including the locking of PCs when not in use; not using or allowing/encouraging pupils or other staff members to use machines logged on by another; and ensuring that no personal data is publicly displayed.

SQA Processes

It is recognised that materials have to be sent to SQA on USB Devices. To minimise risk of data breach it is recommended that encrypted and password protected devices are used (the return of these by SQA can be requested), with the password sent by follow-up email to the relevant person in SQA.

Pupils

It is important that pupils learn the importance of network and data security. Pupils should not have access to sensitive data but the network security risk still applies. **Pupil use of personal USB devices is strongly discouraged**. The use of One Drive (DCC or Glow) must be encouraged instead. Any personal USB device used **must be secure, encrypted and password protected.**

Large Storage Devices (e.g. External Hard Drives used by some secondary departments, Early Years teams, Accessibility and Inclusion teams and others)

External storage devices used **for curriculum purposes and in school only** must have clear processes in place for keeping the device secure which have been shared and agreed with the school's Senior Leadership Team. These processes should include encryption and password protection; passing on of passwords when appropriate (e.g. if a staff member moves on); sign in/sign out systems; and actions to be taken if a device goes missing.

Any new devices purchased must have an encryption and password protection facility, and should be purchased through IT Procurement. From August 2021, only devices which are fully encrypted and password protected may be used on the curriculum network.

External storage devices should not be used outwith school e.g. by staff at home.

Visitors

Visiting presenters and workshop leaders should also be strongly discouraged from using USB devices. If used, these **MUST be secure, encrypted and password protected**. Visitors could share presentations in advance or use cloud storage. The staff member arranging a visit is responsible for ensuring compliance and relevant virus scanning.

Future:

No personal USB storage devices will be permitted on the curriculum network from **August 2022** (any GDPR breaches in the interim would lead to this timescale shortening).

Policy produced: February 2020 **Review: August 2021**

Corporate IT Policy Extract:

Section 12

USB Memory Devices

The council discourages the use of USB memory sticks. Employees should avoid their use wherever possible.

Their small physical size, speed and ever-increasing storage capacity make USB memory devices a convenient device to use for transferring information from one place to another. However, these very features introduce new security risks and amplify risks that already existed with floppy disks.

The primary risks associated with USB memory sticks are:

- Virus Transmissions - Data sharing opens up an avenue for viruses to propagate;
- Corruption of data - Corruption can occur if the drive is not un-mounted cleanly;
- Loss of media - The device is physically small and can easily be misplaced;
- Loss of confidentiality – Data on the lost physical media can be obtained by others.

To mitigate these risks, these devices should be used sparingly and where they are used, the following must be adhered to:

- USB memory devices should generally be used only to transfer non-sensitive, non-confidential information.
- If sensitive, confidential information has to be transferred by this medium assistance must be sought from IT.
- These devices should only be used for occasional transfer of information. If regular transfer of information is required then a request must be sent to the IT Service.
- Once the transfer is complete then the information must be removed from the device.
- If the device is used on non-council equipment then it must be virus checked on return to the council even if all information has been removed.
- If a device is misplaced/lost then this must be reported immediately to the IT Services' Help Desk on One Dundee or via ext 8000, stating what information is on the device.