Nottinghamshire County Council

Removable Media Usage Policy

TO ALL IT USERS

"Nottinghamshire County Council (NCC) continues to place increasing reliance on its computer systems and networks.

Everyone within NCC has a responsibility to control risk and to report errors in judgement or procedure where they see them. Doing so reduces our exposures and helps to maintain our client image.

This policy document has been agreed by the ICT Executive Group and approved by the County Council. It outlines your responsibilities in respect of the computer systems you use. Adherence to it is each person's individual responsibility."

Wilful or negligent disregard for these policies will be investigated and may be treated as a disciplinary matter.

Mick Burrows

Chief Executive

Removable Media Usage Policy

Intent

There are many forms of computer-readable data storage media, some of which allow the medium containing data to be removed from the PC in order to transport the data to another location or another system. The intent of this policy is to secure data held on removable media such that it will not be used in any unauthorised way. The policy is also intended to reduce the risk of infection of corporate systems by viruses carried on removable media.

Scope

The policy applies to all media that can be used to transport data outside of a computer system. This includes but is not limited to floppy disks, CDs and DVDs, PC cards, all types of flash memory cards, PDA's holding corporate data and portable hard disk drives.

Removable media are normally recognised as "external drives" and assigned a drive letter. The policy covers all such devices, and any which are not recognised under a drive letter are not included and may not be used without further investigation by IT.

The policy relates to information which is classified under the Data Classification Policy as Sensitive, Confidential or Critical.

Key Issues

- Many forms of removable media are very small, so loss of the medium is a significant risk.
- Removable media are meant to be transported between systems, so spreading of virus infections is a significant risk.

Objectives

- To preserve the integrity of NCC information and services;
- To reduce (to an acceptable level) the risk of serious financial loss, loss of client confidence or other serious operational or business impact as a result of a failure in data security;
- To comply with all relevant legislation, including that dealing with data protection and (where applicable) to ensure that NCC is protected under computer misuse legislation;

- To satisfy all relevant regulatory requirements imposed on NCC;
- To minimise the risk of propagating viruses via removable media.

Policy

All information used for business purposes should preferably be held on devices that are permanently connected to the corporate network. This enables all security, backup and recovery facilities to operate effectively.

Where there is a business need, information may be transported on removable media subject to the guidelines given below.

Information which is classified as Sensitive, Confidential or Critical (as defined within the Data Classification Policy) may only be written to removable media with the agreement of the relevant data owner (or someone delegated by the data owner).

Information which is classified as Confidential, Sensitive or Critical and which is to be carried outside NCC premises on removable media must be held in an encrypted form. Password protection of files gives a simple method of encryption using the password as a hashing key, and is sufficiently secure for NCC's purposes. Naturally the password may not be written on the media that also contains the encrypted files.

The corporate tool for avoidance of virus infection is Sophos Anti-Virus, which is subject to frequent automated update requiring no user intervention. Where removable storage media have been mounted on any device not protected by Sophos, it is essential that they be virus-checked immediately on connection to any corporate system. The user must run Sophos Anti-Virus manually on the connected device (Start / Programs / Sophos Anti-Virus / Sophos Anti-Virus / select appropriate drive letter / Go button).

In the event of loss of any removable media containing files classified as Sensitive, Confidential or Critical, the user should inform their manager and the IT Security Manager.

Where removable media are to be disposed of, this must be done in compliance with the Policy for Disposal of Storage Media.

Exceptions

Storage media containing only data classified as Public need not comply with this policy.

Any further exceptions to the agreed policy must be authorised by the IT Security Manager.

Responsibilities

Heads of Business Area or delegated **Authorisers** are responsible for providing clear authorisation for all use of removable media within their area of responsibility.

Data Owners or someone delegated by the data owner are responsible for confirming whether transfer of data to removable media is permitted.

Security Administrators will ensure that removable media are used in accordance with authorisations and with this policy.

The **IT Security Manager** will propose policy, provide specialist support and advice to the business and undertake independent monitoring of security (including audit trail analysis).

All Managers are responsible for ensuring compliance with policy by themselves and all their staff. In particular, Managers must ensure that their staff are aware of all policies and associated guidelines/standards.

All Users of removable media are responsible for complying with this policy. They must notify management of security incidents (such as loss of media) and of any known security breaches.