Corporate Information Governance Group

Information Governance Policy Framework

Removable Media Policy

Contents:

Corporate Information Governance Group.
Removable Media Policy

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the Councils, Councillors, Employees, Partners, contractual third parties and agents of the Councils.

Removable Media

Background

The Councils' recognise that there are genuine and potentially significant risks associated with the use of Removable Media.

This policy aims to ensure that the use of removable media devices is duly considered, controlled and authorised.

This policy aims to mitigate the following risks:

- The loss of information, regardless of cause; i.e. through theft, loss or negligent use of removable media devices.
- Infection of Council networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Potential sanctions against the Council or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the Council or individuals as a result of information loss or misuse.
- Council reputational damage as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

A removable media device is any device or medium capable of transporting data, so includes, but is not restricted to the following:

- iPhones/smart phones
- iPads/tablets
- CDs/DVDs
- Optical Disks
- External Hard Drives
- USB Memory Sticks (also known as pen drives or flash drives)
- Media Card Readers
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards)

- MP3 Players
- Digital Cameras
- Backup Cassettes
- Audio Tapes (including Dictaphones and Answering Machines)

Key Messages

- Avoid the use of removable media wherever possible.
- Data stored on removable media devices must be encrypted.
- Data may only be temporarily stored on removable media; it must not be the only copy.
- Removable media devices that are no longer required, or have become damaged, must be handed to ICT.
- Returning or Visiting removable media must be scanned by ICT before being connected to council equipment.
- USB Storage (pen or disk drives etc.) must be procured via ICT.
- If in doubt, seek advice.

Policy Detail

Use of Removable Media presents some significant challenges to the Confidentiality, Integrity and Availability of the council's digital assets. This policy sets out guidance so that when removable media must be used, it is used safely and in compliance with the law.

The recommendation is that removable media is not used and that alternatives should be favoured whenever possible. However, the councils recognise that there are times where its use is the only practical solution. This policy sets out what measures must be taken to protect the council's digital assets where the use of removable media cannot be avoided.

Removable media is a catch all term for a range of devices and technologies. Some protection measures outlined in this policy may not apply to all devices. You should exercise your common sense in the use of removable media, if you are unclear at any point, seek advice from ICT.

Use of removable media is monitored.

Avoid the use of removable media wherever possible.

There are many ways to transfer data without using removable media; Email is the most common and recommended method, especially for smaller data sets. For larger data sets, shared regularly, there are varying options across the councils such as Citrix Sharefile and Corporate Google storage. If you are unsure what options are available to you, please contact the ICT Service Desk for details.

For sharing and collaboration within the organisations, a folder on the shared network is appropriate. Contact the ICT service desk about establishing a safe shared location on the "R" Drive as this storage location is available across the partnership. Do not attempt to create you own R Drive folder, as this would be open to everyone to access.

Corporate Information Governance Group.
Removable Media Policy

If you need to work on a document at home, use your work laptop and Citrix. Remember you are not allowed to connect your own personal removable media device to council equipment, and you should not be accessing council systems from a personal device.

There may be genuine operational reasons to store personal or sensitive information on your laptop hard drive i.e. for Business Continuity; this must always be maintained at the current version. If the information can reasonably be accessed via normal remote working tools, then this should be the default method.

Taking documents home on a USB Stick to work on, on your home computer is expressly prohibited. Similarly, you must not email documents to a personal email address or use personal Cloud storage solutions e.g. OneDrive or Google Drive.

You are strongly advised never to save files containing personal or sensitive data to removable media, where this is unavoidable you should contact the ICT Service Desk for advice.

Council data must remain on and only be accessed by council approved equipment.

You are encouraged to seek advice from the ICT Service Desk about alternative solutions.

Data stored on removable media devices must be encrypted.

Removable media can be lost or stolen; if that happens the data on it is at risk. The Data Protection Act requires that you take reasonable steps to protect personal and sensitive data.

This is where the requirement for data encryption arises. This way, if the device is lost, the only loss is the physical device - the data is not considered as having been compromised.

Losing data could result in a fine of up to £500,000, damage to the council's reputation and be damaging for any individuals affected by the loss. By encrypting that data we are removing that risk.

A printed document is media that is removable but encrypting a piece of paper would obviously not be practical. An appropriate measure could be to place it in a sealed envelope and sent by a "signed for" service.

Digital media must always be encrypted. If you need advice about this, contact the ICT service desk.

Data may only be temporarily stored on removable media; it must not be the only copy.

If there is only one copy of the data and it's stored on removable media, there is a risk that data will be permanently lost if that media breaks. All council data should be stored on the network and copies transferred to the removable media.

Corporate Information Governance Group.
Removable Media Policy

Much of the council's data is subject to the Freedom of Information Act. If we hold the information, we are obliged to produce it if requested. Similarly, a citizen may make a Subject Access Request [part of the DPA]. If that data is not stored on the network, it cannot be found by a search and we would be in breach of these legal obligations.

Returning or Visiting removable media must be scanned by ICT before being connected to council equipment.

Sometimes, removable media from outside our organisation is brought in and needs to be used. Perhaps a contractor has some data on a CD, or a visitor has brought in a presentation on a USB stick. In this case, it's important to have that scanned by ICT before it's connected.

All digital removable media has the ability transfer computer viruses between the devices they visit [are connected to]. It's possible that even your council approved USB stick could become infected, if it has visited something that's infected. Perhaps you took a presentation to another organisation and it was plugged into the laptop that drives the projector. For this reason any "returning" removable media also needs to be scanned.

Other UK local authorities have suffered £500,000 losses and had to shut down their networks for weeks to resolve virus infections, please take the time to contact the ICT Service Desk.

Responsibilities

All staff are responsible for:

- Only using devices supplied/approved by ICT.
- Securely handling and storing removable media devices.
- Ensuring that all data stored on removable media devices is encrypted.
- Contacting ICT if a removable media device is damaged or faulty.
- Removing all data from the device as soon as practical and prior to disposal.
- Returning devices to ICT when they are no longer needed.
- Reporting any actual or suspected breaches via the Incident Management Process promptly after they are noticed.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Council's disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Removable Media
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
21/03/2016	Sophie Chadwick Tim Howes	1.0	First Draft for Consideration
23/09/2016	CIGG	1.1	Final Review
28/9/2016	Will Causton	1.2	Redrafting following review