Parish Office, Sports Pavilion, Hundred Acre Way, Red Lodge, Suffolk, IP28 8FQ

Removable Media Policy

Contents

Document Control		3
Document Amendment History		3
1	Purpose	4
2	Scope	4
3	Advice and Assistance	5
4	Responsibilities	5
5	Incident Management	5
6	Data Administration	5
7	Security	6
8	Use of removable media	6
9	Faulty or Unneeded Storage Devices	7
10	Requests to suspend this policy	7
11	Breach procedures	7
12	Review And Revision	7
13	Key Messages For Staff	8

Document Control

Organisation	
Title	
Creator	
Source	
Approvals	
Distribution	
Filename	
Owner	
Subject	
Protective Marking	
Review date	

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description

1 Purpose

1.1 This policy supports the controlled storage and transfer of information by Councillors of Red Lodge Parish Council and all employees, temporary staff and agents (contractors, consultants and others working on behalf of the Council) who have access to and use of computing equipment that is owned or leased by Red Lodge Parish Council.

1.2 Information is used throughout the Authority and is sometimes shared with external organisations and applicants. The use of removable media may result in the loss of the ability to access information, or interference with the integrity of information, which could have a significant effect on the efficient operation of the Authority and may result in financial loss and an inability to provide services to the public.

1.3 It is therefore essential for the continued operation of the Authority that the availability, integrity and confidentiality of all storage devices are maintained at a level which is appropriate to the Authority's needs.

1.4 The aims of the policy are to ensure that the use of removable storage devices is accomplished with due regard to:

1.4.1 Enabling the correct data to be made available where it is required
1.4.2 Maintaining the integrity of the data
1.4.3 Preventing unintended consequences to the stability of the computer network
1.4.4 Building confidence and trust in data that is being shared between systems
1.4.5 Maintaining high standards of care towards data and information about individual citizens, staff or information that is exempt from disclosure
1.4.6 Compliance with legislation, policies or good practice requirements

2 Scope

2.1 This policy sets out the principles that will be adopted by the Council in order for material to be safely stored on removable media so that the risk of loss or corruption to work data is low.

2.2 Removable media includes but is not limited to:

USB memory sticks, memory cards, portable memory devices, CD / DVDs, diskettes and any other device that transfers data between systems, or stores electronic data separately from email or other applications.

2.3 The Policy does not apply to the use of ICT equipment used in schools for curriculum purposes, but does apply to ICT used for school administration purposes.

2.4 Any person who intends to store Council data on removable media must abide by this Policy. This requirement devolves to Councillors, employees and agents of the Council, who may be held personally liable for any breach of the requirements of this policy.

2.5 Failure to comply with this policy could result in disciplinary action.

3 Advice and Assistance

3.1 The Information Security Manager or equivalent will ensure that everyone that is authorised to access the Authority's information systems is aware of their obligations arising from this policy.

3.2 The IT Service Desk or equivalent should be consulted over any hardware or system issues. The training section should be approached for advice and guidance on using software packages.

3.3 Should this policy appear to conflict with any other approved Council policy, then contact the Information Manager or equivalent for guidance.

4 Responsibilities

4.1 Chief Officers are responsible for enforcing this policy and for having arrangements in place to identify the location of all data used in connection with Council business.

4.2 Users of removable media must have adequate Records Management / Information Security training so that relevant policies are implemented.

5 Incident Management

5.1 It is the duty of all employees and agents of the Council to not allow storage media to be compromised in any way whist in their care or under their control. There must be immediate reporting of any misuse or irresponsible actions that affect work data or information, any loss of material, or actual, or suspected breaches in information security to Community Action Suffolk IT Service Desk.

5.2 It is the duty of all Councillors to report any actual or suspected breaches in information security to the Chief Executive.

6 Data Administration

6.1 Removable media should not be the only place where data created or obtained for work purposes is held, as data that is only held in one place and in one format is at much higher risk of being unavailable through loss, destruction or malfunction of equipment, than data which is routinely backed up.

6.2 Where removable media is used to transfer material between systems then copies of the data should also remain on the source system or computer, until the data is successfully transferred to another computer or system.

6.3 Where there is a business requirement to distribute information to third parties, then removable media must only be used when the file cannot be sent or is too large to be sent by email or other secure electronic means.

6.4 Transferring material to removable media is a snapshot of the data at the time it was saved to the media. Adequate labelling must be undertaken so as to easily identify the version of the data, as well as its content.

6.5 Files must be deleted from removable media, or the removable media destroyed, when the operational use of the material has been completed. The Council's retention and disposition schedule must be implemented by Councillors, employees, contractors and agents for all removable media.

7 Security

7.1 All storage media must be kept in an appropriately secure and safe environment that avoids physical risk, loss or electrical corruption of the business asset. Due to their small size there is a high risk of the removable media being mislaid lost or damaged, therefore special care is required to physically protect the device and the data. Anyone using removable media to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

7.2 Virus Infections must be prevented from damaging the authority's network and computers. Virus and malware checking software approved by Community Action Suffolk IT Services Department must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned by the virus checking software, before the media is loaded on to the receiving machine.

7.3 Any memory stick used in connection with Council equipment or to store Council material should usually be Council owned and be on the Community Action Suffolk IT Services Department approved list. However, work related data from external sources can be transferred to the Council network using memory sticks that are from trusted sources and have been checked using current anti-virus software.

7.4 The Council will not provide support or administrator access for any non-council memory stick.

8 Use of removable media

8.1 Care must be taken over what data or information is transferred onto removable media. Only the data that is authorised and necessary to be transferred should be saved on to the device.

8.2 Material that is classified as RESTRICTED or higher must not be stored on removable media at any time.

8.3 Council material belongs to the Council and any equipment on which it is held should be under the control of the Council and not available to be used for other purposes that may compromise the data.

8.4 All data transferred to removable media should be in accordance with an agreed process established by the Directorate so that material can be traced.

8.5 The person arranging the transfer of data must be authorised to make use of, or process that particular data.

8.6 Whilst in transit or storage the data must be given appropriate security according to the type of data and its sensitivity.

8.7 Encryption must be applied to the data file unless there is no risk to the Council, other organisations or individuals from the data being lost whilst in transit or storage. If encryption is not available, then password control must be applied if removable media must be used for the business purpose.

9 Faulty or Unneeded Storage Devices

9.1 Damaged or faulty media must not be used. Community Action Suffolk IT Services Department must be consulted over any damaged equipment, peripherals or media.

9.2 All unneeded or faulty storage devices must be sent to the Community Action Suffolk IT Services Department who will securely remove the data before reallocating or disposing of the device.

10 Requests to suspend this policy

10.1 This Policy is designed to protect Council business data and to accommodate the needs of users. However, should aspects of this policy interfere with a valid business requirement; an application can be made to Red Lodge Parish Council for an amendment to this policy. An outline risk assessment should be submitted with the application.

11 Breach procedures

11.1 Users who do not adhere to this policy will be dealt with through the Council's, or school's disciplinary process.

11.2 For Councillors, Jayne Cole in association with the Chief Executive will ensure appropriate action is taken.

11.3 Where external service providers, agents or contractors breach the policy, this should be addressed through contract arrangements.

11.4 Where the public have access to the Red Lodge Parish Council system, that access will be withdrawn if there is an actual or likely breach of information security, until adequate controls are in place.

12 Review and Revision

12.1 This policy will be reviewed annually by the Clerk/Red Lodge Parish Council and revised according to developments in legislation, guidance, accepted good practice and operational use.

13 Key Messages for Staff

13.1 Data and information are valuable and must be protected.

13.2 Do not use removable media for material that is marked ‘restricted’ or above.

13.3 Only transfer data onto removable media, if you have the authority to do so.

13.4 All transfer arrangements carry a risk to the data.

13.5 Run the virus checking program on the removable media each time it is connected to a computer.

13.6 Only use approved products for Council data.

13.7 Activate encryption on removable media wherever it is available and password protection if not available

13.8 Data should be available for automatic back up and not solely saved to removable media.

13.9 Delete files from removable media, or destroy the media, after the material has been used for its purpose.

13.10 Ask your manager if you are unsure.