MAULDEN PARISH COUNCIL
Removable Media Policy

Adopted: May, 2018
Next Review Date: Annually

1 PURPOSE

1.1 This policy supports the controlled storage and transfer of information by Councillors of Maulden Parish Council (MPC) and all employees, temporary staff and agents (contractors, consultants and others working on behalf of MPC) who have access to and use of computing equipment that is owned or leased by MPC.
1.2 Information 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 MPC and may result in financial loss and an inability to provide services to the public.
1.3 It is therefore essential for MPC's continued operation that the availability, integrity and confidentiality of all storage devices are maintained at a level which is appropriate to their needs.
1.4 The policy aims 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 MPC 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 Any person who intends to store MPC data on removable media must abide by this policy. This requirement devolves to MPC Councillors, employees, contractors, and agents, who may be held personally liable for any breach of the requirements of this policy.
2.4 Failure to comply with this policy could result in disciplinary action.

3 ADVICE AND ASSISTANCE

3.1 MPC's Clerk will ensure that everyone that is authorised to access MPC's information systems is aware of their obligations arising from this policy.
3.2 MPC's Clerk 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 MPC policy, then contact MPC's Clerk for guidance.

4 RESPONSIBILITIES

4.1 MPC's officers are responsible for enforcing this policy and for having arrangements in place to identify the location of all data used in connection with MPC business.
4.2 Users of removable media must have adequate records management and/or information security training so that relevant policies are implemented.

5 INCIDENT MANAGEMENT

5.1 It is the duty of all MPC Councillors, employees, contractors, and agents to not allow storage media to be compromised in any way while 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 MPC's Clerk.
5.2 It is the duty of all MPC Councillors, employees, contractors, and agents to report any actual or suspected breaches in information security to MPC's Clerk.

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. MPC's retention and disposition schedule must be implemented by MPC 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 MPC's network and computers. Virus and malware checking software approved by the Clerk 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 MPC equipment or to store MPC material should usually be MPC-owned. However, work-related data from external sources can be transferred to the MPC network using memory sticks that are from trusted sources and have been checked using current anti-virus software.
7.4 MPC will not provide support or administrator access for any non-MPC memory stick.

8 USE OF REMOVABLE MEDIA
8.1 Care must be taken over what data or information is transferred on to 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 MPC material belongs to MPC, and any removable media on which it is held should be under the control of MPC 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 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 While 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 MPC, other organisations, or individuals from the data being lost while 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. MPC's Clerk must be consulted over any damaged equipment, peripherals or media.
9.2 All unneeded or faulty storage devices must be sent to MPC's Clerk 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 MPC 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 MPC's Clerk 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 MPC's disciplinary process.
11.2 For MPC Councillors, MPC's Clerk in association with MPC's Chair 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 MPC's system, that access will be withdrawn if there is an actual or likely breach of information security, until adequate controls are in place.

12 KEY MESSAGES FOR MPC COUNCILLORS AND STAFF
12.1 Data and information are valuable and must be protected.
12.2 Do not use removable media for material that is marked 'restricted' or above.
12.3 Only transfer data on to removable media if you have the authority to do so.
12.4 All transfer arrangements carry a risk to the data.
12.5 Run the virus-checking programme on the removable media each time it is connected to a computer.
12.6 Only use approved products for MPC data.
12.7 Activate encryption on removable media wherever it is available and password protection if not available
12.8 Data should be available for automatic back-up and not solely saved to removable media.
12.9 Delete files from removable media, or destroy the media, after the material has been used for its purpose.
12.10 Ask MPC's Clerk if you are unsure.