VILLAGE OF EMPRESS	
Title: Removable Media Device Policy	Policy Number: 12-14
Effective Date: November 2018	Review Date:

Removable Media Device Policy

Intent

This policy supports the controlled storage and transfer of information by Village and all employees, temporary staff and agents (contractors, consultants and others working on behalf of the Village) who have access to and use of computing equipment that is owned or leased by Stone Town Village.
Information is used throughout the Village and is sometimes shared with external organizations 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 Village and may result in financial loss and an inability to provide services to the public.
It is therefore essential for the continued operation of the Village that the availability, integrity and confidentiality of all storage devices are maintained at a level which is appropriate to the Village's needs.

Scope

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

a. Enabling the correct data to be made available where it is required
b. Maintaining the integrity of the data
c. Preventing unintended consequences to the stability of the computer network
d. Building confidence and trust in data that is being shared between systems
e. Maintaining high standards of care towards data and information about individuals, staff or information that is exempt from disclosure

Compliance with legislation, policies or good practice requirements

Definition

For the purposes of definition, the following items shall fall under the category of removable media:

- Flash (Jump) Drives and flash memory storage
- SD Storage
- Removable fixed drives and portable caddies
- R/W Compact Disk or DVD media
- USB remote storage devices

Guidelines

RESPONSIBILITIES

- The CAO is responsible for enforcing this policy and for having arrangements in place to identify the location of all data used in connection with Village business.
- Users of removable media must have adequate training so that relevant policies are implemented.

INCIDENT MANAGEMENT

- It is the duty of all employees and agents of the Village 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 the clerk.
- It is the duty of all Village Employees to report any actual or suspected breaches in information security to the CAO.

DATA ADMINISTRATION

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

SECURITY

- 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.
- Virus Infections must be prevented from damaging the Village s network and computers. Virus and malware checking software approved by the Village, 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.
- Any memory stick used in connection with Village equipment or to store Village material should usually be Village owned. However work related data from external sources can be transferred to the Village network using memory sticks that are from trusted sources and have been checked using current anti-virus software.
- The Village will not provide support or administrator access for any non-Village memory stick.

USE OF REMOVABLE MEDIA

- Care must be taken over what data or information is transferred onto removable media. Only the data that is authorized and necessary to be transferred should be saved on to the device.
- Village material belongs to the Village and any equipment on which primary records are held should be under the control of the CAO and not available to be used for other purposes that may compromise the data.
- The person arranging the transfer of data must be authorized to make use of, or process that particular data.
- Whilst in transit or storage the data must be given appropriate security according to the type of data and its sensitivity.
- Encryption must be applied to the data file unless there is no risk to the Village, other organizations 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.

FAULTY OR UNNEEDED STORAGE DEVICES

- Damaged or faulty media must not be used. The CAO must be consulted over any damaged equipment, peripherals or media.
- All unneeded or faulty storage devices must be dealt with securely to remove the data before reallocating or disposing of the device.

BREACH PROCEDURES

- Users who do not adhere to this policy will be dealt with through the Village disciplinary process.
- Where external service providers, agents or contractors breach the policy, this should be addressed through contract arrangements.

REVIEW AND REVISION

This policy will be reviewed and revised as required by the Village's policy review timetable, or if required as a result of developments in legislation, guidance, accepted good practice and operational use.

EMPLOYEE GUIDE IN BRIEF

- Data and information are valuable and must be protected.
- Only transfer data onto removable media, if you have the authority to do so.
- All transfer arrangements carry a risk to the data.
- Run the virus checking program on the removable media each time it is connected to a computer.
- Only use approved products for Village data.
- Activate encryption on removable media wherever it is available and password protection if not available
- Data should be available for automatic back up and not solely saved to removable media.
- Delete files from removable media, or destroy the media, after the material has been used for its purpose.

Acknowledgement & Agreement

I, , acknowledge that I have read and understand the Telecommunications Policy of the Village of Empress. I agree to adhere to this policy and will ensure that employees working under my direction adhere to this Policy. I understand that if I violate the rules set forth in this Policy, I may face disciplinary action, up to and including termination of employment.

Name: _____

Signature: _____

Date: _____

Witness: _____