The Management of Transferable Data Policy

Purpose

1.1 This policy supports the controlled storage and transfer of information by Councillors and all employees, temporary staff and agents (contractors, consultants and others working on behalf of the Parish Council) who have access to and use of any computing equipment that is owned or leased by Headley Parish Council. It also includes the use of any other computing equipment that may be used by any of the afore mentioned in carrying out appropriate tasks, for which they have been requested.

1.2 Information is used throughout the Parish Council 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. This could have a significant effect on the efficient operation of the Parish Council 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 Parish Council that the availability, integrity and confidentiality of all storage devices are maintained at a level which is appropriate to the Council's needs.

1.4 The aims of the policy are to ensure that the use of removable storage devices, which includes laptops and other appropriate systems, is accomplished with due regard to:

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

Principals

2.1 This policy sets out the principles that will be adopted by the Parish 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
- Laptops and other associated systems
- It also includes 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 Parish Council data on removable media must abide by this Policy. This requirement devolves to Councillors, employees and agents of the Parish Council, 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 and/or legal action.

Advice and Assistance

3.1 The Clerk & Executive Officer will ensure that everyone that is authorised to access the Parish Council's information systems is aware of all their obligations arising from this policy.

3.2 A competent person should be consulted over any hardware or system issues. Advice and guidance on using software packages should also be sought from a competent person.

4 Responsibilities

4.1 The Clerk & Executive Officer is responsible for enforcing this policy and for having arrangements in place to identify the location of all data used in connection with Parish Council business.

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

Incident Management

5.1 It is the duty of all employees and agents of the Parish Council not to allow storage media, including laptops etc., to be compromised in any way whist in their care or under their control. There must be immediate reporting of any misuse of actions that affect work data or information, any loss of material, or actual, or suspected breaches in information security should be reported to the Clerk & Executive Officer. The loss of material is not restricted to just software but also includes hardware and also any paper information.

5.2 It is the duty of all Councillors/Employees to report any actual or even suspected breaches of information security to the Clerk & Executive Officer.

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 Parish Council's retention and disposition schedule must be implemented by Councillors, employees, contractors and agents for all removable media, and confirmed in writing that it has been done so.

Security

7.1 All storage media, including laptops etc., 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 Parish Council's network and computers. Virus and malware checking software approved by the Council, 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 or laptop etc., used in connection with Parish Council equipment or to store Parish Council material should usually be Parish Council owned. 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 Parish Council will not provide support or administrator access for any non-council memory stick or laptop etc.

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

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

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

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

8.6 Encryption must be applied to the data file unless there is no risk to the Parish 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.

Faulty or Unneeded Storage Devices

9.1 Damaged or faulty media must not be used. The Clerk & Executive Officer must be consulted over any damaged equipment, peripherals or media.

9.2 All unneeded or faulty storage devices must be dealt with securely to remove the data before reallocating or disposing of the device. If the device is to be disposed of then it must be ensured that the appropriate device is securely disposed of. A quick format is NOT sufficient.

Breach procedures

10.1 Users who do not adhere to this policy will be dealt with through the Parish Council's disciplinary process and this may result in legal action.

10.2 Where external service providers, agents or contractors breach the policy, this should be addressed through contract arrangements, and may result in legal action.

Review and Revision

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

Employees Guide in Brief

12.1 Data and information are valuable and must be protected at all times.

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

12.3 All transfer arrangements carry a risk to the data.

12.4 Always run the virus checking programme on the removable media each time it is connected to any computer.

12.5 Only use approved products for Parish Council data.

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

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

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

12.9 Appropriate and approved encryption programs are available from the Clerk & Executive Officer.