This report will be made public on 25 April 2016

Folkestone
Hythe & Romney Marsh
Shepway District Council
www.shepway.gov.uk

Report number **A/16/09**

To: **Council**
Date: **4 May 2016**
Status: **Non-Executive Decision**
Head of Service: **Jeremy Chambers, Corporate Director Resources**

SUBJECT: **DIGITAL TRANSFORMATION - ICT FOR MEMBERS**

SUMMARY:

Shepway District Council is embarking on a series of digital transformation projects that will facilitate modern and efficient working, improve accuracy, and create savings through the increased adoption of technology. In addition, using such technology projects a better image to customers who would expect the council to be adopting smarter working practices in order to better serve its citizens. In line with this agenda, the Council has an ambition to assist its Members embrace digital transformation to enable faster and more convenient access to information in order for them to more easily and effectively carry out their roles. It is proposed that Members are offered the use of a Council-owned tablet computer.

However with the benefits technology can bring to the workplace there are increased risks to information that is held electronically and increased requirements to comply with legislation and other guidance, therefore some practices such as the automatic forwarding of council emails to potentially insecure mail accounts needs to be reviewed and the adoption of a tablet solution helps in part to address the security concerns about out dated practices.

REASONS FOR RECOMMENDATIONS:

Preparing, printing and issuing committee documents and reports for Members is both expensive and resource intensive. Many councils are moving towards electronic working for members including providing tablet computers. It is recommended that the practice of issuing the bulk of routine committee documents in a paper format to councillors be replaced as far as possible by moving to electronic documentation and digital working enabled through the provision of tablet computers.

In order to encourage the greater use of digital technology the continued payment of an ICT allowance for members should be dependent upon the actual use of such technology.

The council has recently been challenged over of information security and data handling related to members and it is current difficult to give any degree of assurance that legislation and other best practice are being followed. Issuing tablets will remove the requirement for members to provide their own ICT equipment helping to improve the security of the information the council holds. Members will still be able to choose to use their own ICT equipment though in future they must certify that certain basic security requirements are being met

The practice of automatically forwarding all emails received by the council to a private mailbox is out dated and potentially increases the risks through so called cyber threats to personal information contained in the emails and leaves both the Council and member at risk of breaching data protection laws. Issuing tablets to members will allow them to access their Shepway email more securely and more conveniently. It is recommended that the practice of automatically forwarding all Council emails to private accounts ceases in line with the stance being taken by other councils where this sort of practice was previously allowed.

RECOMMENDATIONS:

1. **To receive and note report A/16/09.**

2. **To approve the recommendation that:**

    a. **Council-owned tablet computers are offered to members for the reasons outlined at paragraph 1.1.**

    b. **The payment of an ICT allowance to members in future is dependent upon the adoption and use of technology, and the opting-out of routinely receiving paper copies of reports, agendas, and other communications from the Council.**

    c. **Members can continue to use their own ICT equipment as well as, or in place of, a council owned tablet but they must certify that they have certain safeguards in place to protect personal information.**

    d. **That the practice of auto forwarding Council email to private email accounts ceases.**

1. PROPOSAL

1.1 To assist Members making the digital transition, it is proposed that Members are offered the use of a Council-owned tablet computer to allow safe and convenient access to electronic committee papers and emails instead of continuing to receive printed papers. Members who do not feel a tablet solution would be suitable for them will still be able to receive printed copies. Implementing a tablet solution provides the following benefits:

a. It is aligned to the Councils overall Digital transformation agenda and the Government's aim of becoming "digital by default".

b. It helps to meet the Council's objective of reducing the amount, and therefore the cost of printing and distributing material.

c. It releases committee administration and other staff such as print room for other duties and helps drive back office efficiency.

d. The proposal offers a cashable saving and a return on the investment in tablets would be realized in less than 2 years compared to the current cost of printing and posting the bulk of committee papers.

e. The tablet solution is more flexible as documents would be accessible anywhere via a Modern.Gov application and would allow members to access email and research information via the internet as well as having the benefit of a tablet available for other reasonable personal use.(Subject to the Council's ICT usage policies.)

f. Members would always have access to the most up to date version of documents and would not have to store paper copies.

g. The security of information is enhanced.

1.2 In line with the Independent Remuneration Panel's recommendations of October 2015, it is proposed that in future Members would qualify for the Members' monthly ICT allowance only if they have opted out of routinely receiving paper copies of documents. Council owned tablets would also be offered only to those members who no longer take paper copies though they would also retain the option of using their own tablet or laptop if they wished, subject to some additional controls described in the guidance in 1.5 below.

1.3 It is recognized that a tablet solution may not suit everyone, for example individuals who have difficulty reading from computer screens. In these cases printed papers would still be made available but the member would not qualify for the ICT allowance. However, when choosing a tablet solution over the printed copies, it should be remembered that tablet computers do have the facility to zoom in to text making the size more comfortable for the reader and it may be possible to use software to read text out loud.

1.4 In certain circumstances, Democratic Services may consider that issuing paper copies of reports would still be advantageous; for example, to overcome the technical difficulties of dealing with very large file sizes. In such cases, certain documents, plans and reports would still be made available in paper format regardless of whether the member had taken the tablet option or not.

1.5 The secure handling and storage of council information remains a priority, so whereas Council owned tablets can be secured in line with current best practice, Members who opt to use their own computers and tablets must undertake to maintain an appropriate level of security on devices used for accessing Council information. Guidance is provided at Appendix A to this report but in brief this would include:

- Maintaining an up to date antivirus solution.
- Applying system and software patches and updates as and when they are released.
- Enabling personal firewalls.
- Maintaining password or other access controls (such as personal identification numbers, or PINs) on devices and accounts.
- Storing documents, emails or other files containing information related to the business of the Council in places where others who are not entitled to the information cannot gain access to them. This applies, for example, when storing documents on a shared computer, and rules out using a joint email account.

  It is proposed that members who wish to use their own devices but who want to opt out of routinely receiving paper copies of documents in order to qualify for the members ICT allowance would be required to sign an "Access Agreement" based on the criteria above before they are granted access to the SDC portal. A copy of the agreement form is at Annex 1 to Appendix A to this report.

1.6 A tablet may provide additional benefits for members as well as being a means of accessing committee documents and email; for example it may be useful for taking notes, photographs and videos and accessing social media or the internet for research in support of their work as a councillor. Personal use in line with the Council's computer use policy would be allowed.

1.7 It is proposed to issue iPad Air 2 tablets with 64GB memory, as having a standard device reduces support costs and they are fairly simple to use although training would be made available to those members who required it. Members will be offered some choice in the device colour and case options.

2.0 Costs and Return on investment

2.1 The cost of an iPad tablet solution for all members would be in the region of £18.5k.

2.2 The cost of printing and posting committee papers is currently in the region of £11,000 broken down as follows:

- Printing paper copies(including officer time) £9700 and
- Costs of postage £1300

therefore the return on investment is estimated to be within 18 months.

2.3 The current ICT Loan scheme will continue to be available to support Members to embrace the Council's digital and paperless transformation.

3. RISK MANAGEMENT ISSUES

3.1 The recommendations in this report address some of the information governance risks faced by the council and elected members related to the handling and storage of personal information.

4. LEGAL/FINANCIAL AND OTHER CONTROLS/POLICY MATTERS

4.1 Legal Officer's Comments (AK)

The legal issues are covered fully in the body of this report.

4.2 Finance Officer's Comments (TM)

This report recommends that the option of tablet computers is made available to all members of the Council. In return members must opt out of receiving information by paper. In addition, the payment of the ICT allowance to members in future will be dependent upon the adoption and use of technology.

Paragraph 2 shows that the estimated initial cost for all members of the tablets is about £18,500. In addition it indicates that printing costs should reduce by about £9,700 per annum and postage costs by £1300 per annum. Therefore, the costs should be covered within 2 years. If some members did not join the scheme, the cost and savings should be reduced in proportion.

The initial cost could be funded from the ICT Reserve. The printing savings need to be included in the Budget Strategy for 2017/18. Any effect on staffing resources should be included in any future staff review.

4.3 Diversities and Equalities Implications

The equalities and diversity implications of this report have been considered.

CONTACT OFFICERS AND BACKGROUND DOCUMENTS

Councillors with any questions arising out of this report should contact the following officer prior to the meeting

Jeremy Chambers, Corporate Director Resources
Telephone: 01303 853263.
Email: jeremy.chambers@shepway.gov.uk

Appendix A - ICT Guidance for Elected Members

1.0 Introduction

1.1 This guidance note has been produced for Elected Members at Shepway District Council to assist in the use, handling and storage of data by Members. The management and security of information, in particular that related to citizens which is considered "personal data" or "personal sensitive data" carries responsibilities both for the council and the individual member. There are various Acts of Parliament such as the Data Protection Act 1998 (DPA), a wide range of guidance from bodies like the Information Commissioner's Office (ICO) and other requirements such as that issued by Central Government bodies (e.g. HMRC, Cabinet Office) related to the handling and transmission of information all which make can compliance difficult. At the same time the risks to information held and processed electronically are on the increase.

1.2 The Data Protection Act sets out various responsibilities for people who control information. Members are in a unique position in regards to such responsibilities in that sometimes the work they do is directly related to the business of the council in which case the Council is the Data Controller (see definition below). On the other hand they also work as ward members dealing with information on behalf of individual citizens in which case the Member is the Data Controller. The Member may also be working on behalf of a political party in which case the political party is the Data Controller. Those responsibilities can become blurred when a Member is dealing with matters between the Council and individual citizens.

2.0 Data Controllers

2.1 Who is a Data Controller? In essence you are a data controller if you keep or process any information about living people whether that is held on a computer or manual filing system. Being a data controller carries with it serious legal responsibilities, so you should be quite clear if these responsibilities apply to you or the Council. As a guide:

a. The Council is considered to be the data controller when the information is related to the business of the Council.
b. Where a Member is dealing with information on behalf of individual citizens in their capacity as a ward member the responsibility for the management of information rests with the individual Member i.e. the Member is the Data Controller.

2.2 The Data Controller responsibilities do not take account of who owns the equipment and systems where information is contained therefore if a Member has data about a constituent that has been sent to them via their Council email address and they are viewing it on a Council owned computer they are still the Data Controller.

2.3 The problem arises when there is a breach of information security and data is lost. Where the data is contained and processed within the councils systems a

certain degree of control and protection against information loss are provided to mitigate some of the risks associated with the use of computers. If a member is using their own ICT equipment or systems, including their own personal email accounts and cloud storage solutions (such as iDrive, Dropbox) for processing and storing personal data then they must ensure the data protection principles (described below) are applied and that they have adequate safeguards in place not least for their own protection. There are considerable penalties and reputational damage that can arise from non compliance.

3.0 Data protection principles

3.1 The Data Protection Act controls how your personal data is used by organisations, businesses or the government which includes councils and elected members. Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- Used fairly and lawfully
- Used for limited, specifically stated purposes
- Used in a way that is adequate, relevant and not excessive
- Accurate
- Kept for no longer than is absolutely necessary
- Handled according to people's data protection rights
- Kept safe and secure
- Not transferred outside the European Economic Area without adequate protection

4.0 Personal data

4.1 Personal data is information which relates to a living individual who can be identified from that data, or from that data and other information which the Data Controller has access to. Personal data also includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

5.0 Personal Sensitive Data

5.1 Personal Sensitive Data is further information about an individual which could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data and may relate to such things as:

- Race or ethnicity
- Political opinion
- Religious or similar beliefs
- Trade Union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of an offence

- Any proceedings for any offence committed or alleged to have been committed and the disposal of such proceedings or the sentence of any court in such proceedings.

6.0 Securing personally owned computer equipment.

6.1 **General**. Where a member is using privately owned equipment for processing personal data the following guidance should be followed as a minimum:

- Passwords and PINs to lock the device or screen when it is not in use should always be used.

- Different passwords for Council and personal business should always be used. Passwords for council systems should never be shared; not even with ICT staff.

- Passwords should be at least 8 characters in length and contain a mix of upper and lower case letters, numbers and special characters and should not contain common words, family names or part of your user name. Using phrases that are easy to remember are better than single words however long; for example “Mysmalldog1#”.

- If other people have access to the computer you use for your council business (e.g. a family or business computer) there must be separate accounts on the computer for each person and you should log off every time you have finished using it.

- If you lose, or suspect you have lost, Personal information relating to an individual regardless of how it happened e.g. laptop stolen, computer virus you should assess the seriousness of the information getting into the wrong hands and take the following actions:

    - If you have had computer equipment stolen, whether that be personal or council owned, you must report it to the police and obtain a crime report number. This will be required in any insurance claim.

    - If you have lost any council owned equipment you must report it to ICT on 01303 853220.

    - Contact the council’s Compliance and Information Governance Manager on 01303 853444 or the ICT Contracts Officer on 01303 853541 to discuss whether the incident warrants reporting to the Information Commissioners Office.

6.2 Personal computers and laptops. If you are using a personal computer or laptop you should:

- Always have an up-to-date antivirus solution in place. This will always mean having a personal firewall configured on your computer, and will involve either having appropriate anti-virus software installed, or keeping built-in antivirus protection updated. Most commercially available products such as Norton, Kaspersky, McAfee etc provide both levels of protection. They may also have other features such as internet browsing protection, parental controls etc. There are free antivirus products available but the old adage "you get what you pay for" in the internet security world applies.

- Any antivirus product should be configured to automatically scan your computer regularly (weekly) and should also be configured to automatically download and apply the latest updates.

- You should always load security updates provided for the applications on your computer when prompted.

6.3 Tablets and smartphones. There are antivirus products (apps) available for mobile devices (tablets and smartphones) but as they operate in different ways from computers and laptops generally the security of such devices can be managed through the device settings. Apple and Android devices may still be subjected to vulnerabilities though these are usually introduced through cheap or free apps from illicit download sites. The use of an internet security app (such as Webroot) which helps to secure web browsing activities is suggested where appropriate. The biggest risk to information on mobile devices is when the device is lost or stolen. Having said that there are a number of points that should be considered when using mobile devices:

- Always run security and operating system updates when prompted.

- Do not try to bypass the settings in the device (known as jailbreaking).

- Only use apps from reputable sources such as the Apple App Store, Google play store or similar (e.g. Amazon). It is recommended to use apps only from the appropriate Store for the device.

7.0 Email security

Members who process emails related to council business that may contain personal information about employees, other members or citizens should ideally do so in their Shepway email account. This removes many of the compliance requirements from the individual member. The following guidance should be followed:

- Routinely auto forwarding email from one account to another, such as from a Shepway Council email address to a private address presents a risk to the council as there is no control regarding what information is being forwarded. The Council has to ensure that personal data being sent from its own system is adequately protected.

- Keep an email account for Council matters that is separate from work or business, private and family matters. Although this may seem onerous the risk of information leakage is greater when all email is held in one account.

- Have separate passwords for each email account.

- Beware of using “reply to all”, forwarding emails, using the carbon copy (cc) function and distribution lists when forwarding personal data as you must ensure everyone you are sending it to is entitled to receive it.

- Never click links in emails except when you are expecting the email and you recognise the sender (such as when you are expecting a password reset or account activation).

- Be wary of opening attachments you are not expecting.

- Beware of rogue emails trying to gain your personal information (known as Phishing). Some of these emails appear very genuine.

- Many email providers are using web versions of their software for example Hotmail, AOL, Gmail. Many of these are hosted outside the EEA and therefore do not comply with the Data Protection Act. If you are unsure as to where your information is being stored you as a data controller should contact your provider and seek a written assurance regarding where you data is being held.

- Never let other people routinely deal with your Council email on your behalf; they may not be entitled to view the contents.
- When logging out of the Council’s emails (using the Web Portal), take care to ensure no-one can log back in using a user ID and password stored on your computer’s browser.

8.0 File security

8.1 Documents which contain personal information such as letters from constituents or print outs of information should be secured so that they cannot be accessed by people not entitled to see them. This applies whether the document is in paper or

digital format. When dealing with information the following guidance should be followed:

- Personal data and personal sensitive data related to constituents, employees of the Council, or other Members should never be held in an account or storage area that can be accessed by other people.

- Keep separate file structures for council and non-council business.

- Consider password protecting documents.

- If you are storing documents containing personal and personal sensitive data on the hard drive of a computer you should be aware those documents exist even after you have deleted them or formatted the disk so when the computer is no longer required you should ensure the hard drive is physically destroyed.

- If you use a cloud based storage system such as Dropbox, Apple's iCloud, Google Drive, Microsoft One Drive then you need to satisfy yourself that the storage of personal information is compliant.

- Be wary of transferring personal information via USB stick. Apart from the risk of transferring viruses and other malware, they are easy to mislay. If you must use a USB stick to transfer personal information ensure it is of the encrypted type or that the files on the stick are either encrypted or password protected. Do not allow others to use the same stick.

9.0 Social Media

9.1 Using social media channels like Facebook and Twitter pose particular risks for members. The following guidance should be applied when using such channels, as a minimum to protect both your own and the Council's reputation:

- If you maintain a social media presence such as a Facebook account to assist with carrying out your duties as a district councillor you should use a separate account to anything you use for your private life. You should check your profile and security settings regularly to make sure you have the correct levels of privacy for each account.

- You should never use such channels for dealing with personal information or personal sensitive information. If a constituent contacts you via social media you should consider how you need to reply, and possibly advise the person to contact you via email.

- You should be wary of commenting on or expressing any form of opinion about an individual person.

10.0 Wireless hot spots

10.1 The increasing coverage of free public wireless networks means devices can frequently be connected to the internet from many public spaces such as hotels, restaurants airports. However, there are a number of security concerns related to their use:

- You can never be sure if the wireless access point you are connecting to is actually what you think it is, for example anyone with a mobile phone or computer can set up a wireless hotspot in a coffee shop and call it “cafe secure Wi-Fi”.

- You cannot be sure who else is connected to the same network, and whether they can capture your data.

10.2 There are a number of things you can do to reduce the risk when using open Wi-Fi connections:

- If there are secure connections available choose one of these instead.

- Turn of data sharing application and location aware services. Turn on Wi-Fi only when you need it.

- Do not use Shepway’s web portal (for emails or intranet) and avoid using other websites that require you to input a user name and password such as online shopping and banking when connected to an open connection.

11.0 Freedom of Information and Subject Access Requests

11.1 The Council is frequently asked to produce electronic copies of documents and emails in response to Freedom of Information requests and Subject Access Requests. It is important to remember that any correspondence that is sent via the Council may be retrieved and produced for a member of the public who makes such a request and who has a right to such documents. The council currently archives all emails for 3 years but other documents may be kept for longer than that.

12.0 Further reading

Further guidance on the data protection act can be found on the Information Commissioners website https://ico.org.uk/for-organisations/guide-to-data-protection/

The Council’s Information Security Policy and Use of Computers Policy are available on the intranet under ICT Services.

Annex 1 to Appendix A to
Shepway District Council Report A/16/
ICT for Members dated May 2016

Form to request access to appropriate Council information systems from personal ICT equipment. (e.g. Outlook Web Access and Intranet.)

Use of personally owned ICT equipment during municipal year xxxx/yy

This is to certify that I wish to use my own personal ICT equipment for the processing of council information. I have read and understood the ICT guidance for members issued by Shepway District Council and will ensure adequate technical and physical security measures in place to protect the information related to the business of the council. I understand that I may from time to time be asked to provide evidence that appropriate security measures are in place.

Name…….

Sign……

Date……

This form is to be signed annually and to be returned to Committee Services once completed