Agenda Item No: 9

INFORMATION SECURITY REPORT – EMAIL SECURITY

To: **General Purposes Committee**

Meeting Date: **28 November 2017**

From: **Sue Grace, Director of Corporate & Customer Services**

Electoral division(s): **All**

Forward Plan ref: **Not applicable** *Key decision:* ***No***

Purpose: **To consider the Council's Email Policy and Email Security**

Recommendation: **General Purposes Committee is asked to:**

a) **Approve the Email Policy and Personal Commitment Statement and where it is appropriate for Members to sign a personal commitment statement by end of December 2017.**

b) **Mandate for all Members to complete the Member Data Protection course by end of December 2017.**

	Officer contact:		***Member contacts:***
Name:	Dan Horrex	Names:	Councillors Count & Hickford
Post:	BI Manager – Information & Records	Post:	Chair/Vice-Chair
Email:	Dan.horrex@cammbridgeshire.gov.uk	Email:	Steve.Count@cambridgeshire.gov.uk Roger.Hickford@cambridgeshire.gov.uk
Tel:	01223 728416	Tel:	01223 706398

1.0 BACKGROUND

1.1 Information is an important asset to any organisation and it is important that we manage such information both efficiently, effectively, safely and securely. As the majority of our information is managed digitally, IT security must also be considered.

1.2 Over the last few years, organisations globally and governments have been subject to cyber attacks by sophisticated cyber hackers who have been able to secure access to systems which were regarded as very secure (**Appendix A**). Information security incidents can occur for a range of reasons, including fraud as well as forging access through systems known as hacking. We, like many organisations, witness this sort of activity on a regular basis. For instance, email addresses can be spoofed, this is where an address is imitated so that communications can be sent out from an unknown source disguised as someone who is known to the receiver. In a recent example emails were sent out asking recipients for money. This is called phishing and involves fraud through impersonation to gain financial advantage. A report produced by Symantec (an internet security company) stated that email was popular as an attack channel because it does not rely on vulnerabilities in the infrastructure itself but uses simple deception to lure victims into opening attachments, following links and disclosing their credentials.

1.3 As the Council is hit on an hourly basis by phishing and spam attacks we protect ourselves in three ways against these attacks:

- Sophisticated filters which prevent such emails coming through;
- Frequent communication with staff and Members when an attack gets through alerting of the risk;
- Careful monitoring of incoming emails to spot patterns of emails from fraudulent senders so that effective action can be taken.

1.4 Against this background there is both national guidance and legislation which sets a framework for good practice in information security and governance. The main legislation governing this area is the Data Protection Act 1998, and the General Data Protection Regulations (which will be introduced in 2018). Principle 7 of the Data Protection Act states we must keep information secure. Likewise the Council's Information Management Strategy sets out the key principles of effective Information Management. One of these principles is that information should be kept secure.

Information governance/security maintains the following principles:

- Confidentiality – Protecting sensitive information from unauthorised access or disclosure.
- Integrity – Safeguarding the accuracy and completeness of information and processes.
- Availability – Ensuring that information is available to authorised people when needed.

1.5 The Council distils the legislation and guidance into a policy framework and good practice for the safe handling of information. With the acceleration of cyber crime, hacking and phishing, the Council has decided to review these policies with a particular emphasis on the safe handling of information through email correspondence. This paper sets out the findings of the review and action which now needs to be taken to ensure the security of sensitive information contained in emails.

2.0 MAIN ISSUES

2.1 The review looked at a number of factors as follows:

- The security of personal email accounts;
- Compliance with other legislative requirements such as General Data Protection Regulations and Freedom of Information;
- The consequences to the Council and Members of an information security breach.

2.2 Specialist email providers will claim that they can make email accounts secure and whilst a degree of security can be maintained there are a number of factors which mitigate against this as follows:

- Emails sent via Council email are part of a secure email network. Personal email accounts send emails over the open internet in an unsecure form which is readable by others.
- If a personal email account is hacked, it may often initially go unnoticed by the user and the Council will not know either which means that the Council may lose sensitive data with no means of knowing what has been lost and to whom. Logging and monitoring of the Council email account will show when hacking is attempted or is successful.
- There is evidence to suggest that Members are at greater risk of cyber attack as their email addresses are publicised and criminals target these.
- Passwords can be hacked and once hacked there can be access to highly sensitive information of which the Council and sometimes the user has no knowledge. Having a complex password is key to security of an email account.

2.3 The Council has obligations under the Freedom of Information legislation which also applies to emails from personal email accounts. For example, a senior Government Minister was required by the Information Commissioner to disclose emails sent to his personal email address. In his ruling the Information Commissioner urged the Minister and his officials to stop using private email for government business and warned him that the use of private emails and texts should be actively discouraged.

2.4 The consequences of an information security breach can include fines. The Information Commissioner can levy fines now of up to €10m for administrative breaches of our obligations to manage information properly and up to €20m for a serious breach. Substantial fines have been levied on the following organisations:

- London Borough of Lewisham £70,000
- Leeds City Council £95,000
- Stoke-on-Trent City Council £120,000
- Greater Manchester Police £150,000
- Welcome Financial Services £150,000
- Brighton and Sussex University Hospitals NHS Trust £ 325,000
- Talk Talk £400,000

2.5 The Council's network has the following advantages:

- Emails between @cambridgeshire.gov.uk addresses are secure and not accessible without network access;

- Access to the network itself is protected, monitored and can be investigated.

In paragraph 1.3 other measures which protect the Council's network are described.

3.0 The Way Forward

3.1 Workshops have been held with Members to discuss proposals to implement controls which will decrease the likelihood and impact of any cyber attack. These include the following:

- All Members to use secure CCC email for Council business.
- Increased awareness of information security and data protection - a new e-learning course has been produced specifically for Members so they can be aware of information security and data protection issues.
- Members to have CCC laptops issued to them to make access to email and Council information easier and safer.
- Members to access emails on a non-council device via appropriate secure means (e.g. the Blackberry software on a mobile device).

3.2 The feedback from Members was that whilst it is important to maintain the security of emails, there was a need to maintain the convenience of personal email accounts.

3.3 Therefore it is proposed that any Member who uses a personal email account or automatically forwards emails from their CCC account to a personal email account must do the following:

- Sign a Personal Commitment statement which highlights Members' responsibility to keep information secure (**Appendix B**).
- Use controls such as regular password changes, using a strong/complex password and anti-virus software, and to take all other reasonable technical and organisational measures which will enhance the security of the email account.
- Read the Information Security – Member Guide (**Appendix C**).

3.4 It is also proposed that all Members need to complete the Member Data Protection e-learning course, regardless of whether they primarily use a CCC email address or an alternative personal, or any other, email account.

3.5 The Email Policy has been revised to take these proposals into account, and is attached as an appendix to this paper (**Appendix D**).

4. ALIGNMENT WITH CORPORATE PRIORITIES

4.1 Developing the local economy for the benefit of all

There are no significant implications for this priority.

4.2 Helping people live healthy and independent lives

There are no significant implications for this priority.

4.3 Supporting and protecting vulnerable people

The Data Protection Act requires us to protect sensitive information from unauthorised

access or disclosure.

5. SIGNIFICANT IMPLICATIONS

5.1 Resource Implications

The implications of not keeping information secure could result in significant fines being levied on the Council.

5.2 Procurement/Contractual/Council Contract Procedure Rules Implications

There are no significant implications within this category.

5.3 Statutory, Legal and Risk Implications

This paper discusses the statutory framework for information security and enforcement at paragraphs 1.4, 2.3 and 2.4. The proposed changes are intended to limit identified risks around loss of information and unsafe information handling.

5.4 Equality and Diversity Implications

There are no significant implications within this category.

5.5 Engagement and Communications Implications

Workshops were held to discuss this issue with Members as part of the review.

5.6 Localism and Local Member Involvement

There are no significant implications within this category.

5.7 Public Health Implications

There are no significant implications within this category.

Implications	Officer Clearance
Have the resource implications been cleared by Finance?	Yes Name of Financial Officer: Tom Kelly
Have the procurement/contractual/ Council Contract Procedure Rules implications been cleared by the LGSS Head of Procurement?	N/A
Has the impact on statutory, legal and risk implications been cleared by LGSS Law?	Yes Name of Legal Officer: Maria Damigos
Have the equality and diversity implications been cleared by your Service Contact?	Yes Name of Officer: Sue Grace
Have any engagement and communication implications been cleared by Communications?	Yes Name of Officer: Christine Birchall
Have any localism and Local Member involvement issues been cleared by your Service Contact?	N/A
Have any Public Health implications been cleared by Public Health	N/A

Source Documents	Location
Global and Local Risks of Cyber Crime Email Policy Information Security – Member Guide Personal Email Security Commitment	Shire Hall, Castle Hill, Cambridge CB3 0AP