Standards Committee
Report

City of Westminster

To: Members of WCC Standards Committee

From: Ben Goward Chief Information Officer (Interim)

Date: 15th March 2017

Subject: **Governance of Member IT, Data Protection Obligations and Training**

---

1. Summary

Elected Members and the Council both have a legal responsibility to ensure that the Council information they control is stored and used in a legally compliant manner, as defined by the Data Protection Act 1998, and the Freedom of Information Act 2000.

Growth in litigation and fines relating to incorrect use of data (maximum penalty currently £500k, rising to €20m in 2018), growing external cybersecurity risks and the development of new technologies challenge the Council to reconsider current IT governance arrangements, and the guidance and training it provides to Members.

Previously Members were advised to use personal email accounts for all Council correspondence, but continuation of these arrangements may not best meet the legal obligations placed on both parties to safeguard Council data.

An improved approach may be considered which takes into account the three discrete roles each member undertakes, as follows:

Role	Responsibility for data	Best system to use	Rationale
Party member/campaigner/activist	Councillor	Personal email/file system	The Council should not be involved in party affairs
Elected community representative	Councillor & Council	Council Office365	*Ward Members have a duty to secure sometimes sensitive communications from their community. *The Council has a duty to ensure that information sent to ward Members is managed securely and in line with the Data Protection Act 1998 *Office365 fulfils these requirements, and allows Members to use their Council addresses for correspondence
Public Administrator (Cabinet Member, Committee Member etc)	Council	Council Office365	The Council is unambiguously responsible for this data and chooses Office365 as the platform to secure this information

This report provides further information on the above, and focuses on the potential benefits to Members of adopting the recommended approach. It also provides information on the proposed training and support which could be given to Councillors over coming months, and in the run up to the next Elections in 2018.

2. Recommendations

2.1 That the Committee note the contents of this report as the proposed basis of training sessions to be provided for all members.

2.2 That the Committee comment on the proposed changes and advise if any further issues not set out should be included

2.3 That the Committee note that governance information on Member IT is proposed to be included again in the information issued as part of the 2018 Member induction material

3. Reasons for the decision

3.1 Council obligations

The Data Protection Act 1998 places an obligation on the Council to ensure that there is adequate protection for any data it shares with Members. Protection does not just refer to security, but importantly the ability to maintain and access information assets that are ultimately owned by the Council as the primary Data Controller.

As Data Controller the Council has a duty to ensure that the information it provides to those acting on its behalf, such as Members, is kept secure, accessed by those authorised to see it, and is destroyed when no longer needed. The Council cannot devolve its legal responsibilities to a third party; hence where Members are processing Council information the Council remains potentially liable should this processing result in a breach of the Act.

3.2 Member Obligations

Under the Act, Members are also classed as Data Controllers with responsibility for the Council information they handle. All Members are individually registered with the regulator (the Information Commissioners Office, "ICO") – this is undertaken annually by Member services on their behalf and describes the nature of the processing of personal data which councillors will undertake.

Where information is provided by a resident to their elected representative the Member is a Data Controller in their own right and is liable for ensuring the secure handling of this information. Such information should only be kept for as long as is necessary and should be destroyed in a secure and timely manner.

Members may be asked to provide copies of information they hold about an individual. The law states that as a Data Controller they must respond by providing written copies within 40 calendar days. Failure to do so amounts to a breach of the Act. Individuals can complain to the ICO who in turn can impose conditions, including ordering Members to disclose.

3.3 Challenge to existing IT Governance arrangements

Current IT governance arrangements are predicated on a straightforward split between a Member's information handling activities, and those of the Council. Specifically, although all Members have an "@westminster.gov.uk" email address which is advertised on the Council's website, this is typically forwarded to a personal email address (e.g. Yahoo or Hotmail) which is managed by each Member. By auto forwarding emails the Council ensures that Member electronic communications are not captured or stored on the Council's network.

However, whilst this approach had the advantage of keeping Members' party and personal data separate from Council data, it complicates the Council's ability to fulfil its legal obligations (Section 3.1) and places a significant burden of risk on Members. Forwarding emails to personal accounts carries risk because the Council cannot guarantee the adequacy of external webmail services to handle sensitive information.

The expansion of mobile technology has made information sharing easier and quicker, changing the communication landscape for Members, officers and members of the public. However there has been a concurrent expansion in cybercrime, identity theft, hacking, and denial of service risk. These threats require all organisations to re-evaluate the nature of the compliance controls needed to protect personal and other confidential information.

Compliance legislation is attempting to keep abreast of these changes by imposing tougher sanctions, and demanding greater organisational transparency over how information is managed. The obligations placed on Members by laws such as the Data Protection Act mean that they - as well as the council - are responsible for any failure to secure or handle information appropriately.

Penalties for Data Controllers (legal entities and individuals) can reach up to £500,000 under the current regime. However, this is set to rise up to €20m under the new EU General Data Protection Rules [GDPR] which will come into force on 28th May 2018. The UK government has confirmed that the UK decision to leave the EU will not affect the commencement of GDPR.

3.4 Advantages of new IT governance arrangements

During 2016 the Council replaced its legacy email systems with the cloud based Microsoft Office365 technology platform. All email accounts, including those of Members were migrated to this platform. In addition to email, Office365 offers a host of facilities, designed to share and communicate information in one secure place.

This report proposes that training be provided to support the cessation of all existing Member email auto-forwarding. Members will be strongly encouraged to use Office 365 directly to send, receive and store Council data. Members own private correspondence, i.e. party political or personal should continue to be provisioned by Members directly and responsibility remains with Members to find adequate external email provision.

Using Office365 to access Council data has the following advantages:

- The Council will ensure that information provided to Members has the same technical safeguards as all other council information shared with its officers
- Members may securely access their council related email and other electronic records 'anywhere' 'anytime' including documents and notes. The ability for modern mobile devices to open multiple mailbox/accounts means this information may be blended with their personal accounts at point of consumption to provide a "single inbox" experience without compromising data integrity
- Data Protection obligations around storage and retention can be easily applied to council information
- A clear distinction between council activities and private correspondence can be maintained
- Members can share information with confidence as secure encrypted email is a feature of Office365.
- The privacy of Member emails is maintained as the management of such correspondence remains under the purview of Members
- Legal rights of access to council related information can be easily fulfilled enabling both Members and the Council to meet their statutory obligations

- Any information requests under FOI and Data Protection involving Member correspondence can now be managed jointly by the council and Members – that is advice/guidance over the use of exemptions, as well as the editing of information before it is disclosed.
- Both Members and the Council will attain a higher level of compliance assurance and thus significantly reduce the threat of a data breach, through inappropriate sharing or loss of data.

These proposals are in keeping with the legislative requirements and associated penalties which are set to increase under GDPR with respect to information handling by individuals, organisations and public sector bodies.

3.5 Potential for improved training

The Council intends to invite Members to interactive training sessions over the course of the summer 2017 providing practical guidance and advice on understanding how the Data Protection Act impacts on their different roles and responsibilities. The sessions will be run three times over the summer to afford all Members an opportunity to attend. Using real case scenarios, Members will be able to bring to bear their own experience and understanding, as well as be provided with practical tips and solutions on handling council and constituency data.

In addition Members will also be offered practical guidance on managing their Office365 accounts, in relation to storage and email. All such advice and guidance will also be afforded to new Members as part of the induction process.

Training will be based on scenarios covering the different Member roles as follows:

3.5.1 Member/campaigner/activist scenario:

“A council received a complaint notice from the ICO with regard to the use of email. It is alleged that the council has shared email addresses with a Member sitting on a Planning Committee, who had in turn used it to canvass support on behalf of his/her political party during an election year. The Council was able to demonstrate it had not provided ANY email for a non-council purpose, and that as the Member was a Data Controller in their own right, then the complaint should be re-directed to them. The ICO accepted this argument.” Please note the following:

a) Initially the council was deemed responsible. This is because as a Data Controller it has a responsibility to ensure any data sharing is done lawfully. In the above scenario the council would have had to obtain consent from the recipients that their email addresses could be provided to a councillor for party political purposes – without such consent, any actions taken by the *Member* were deemed unlawful.
b) The Member was solely responsible for how this information was handled, i.e. was aware that the information provided was not for the purpose of political campaigning.
c) Any liabilities including fines would be levied at the Member and *not* the council who had given the email addresses for a specified official council purpose. It was the Member and not the council who had gone on to use it for a non-council purpose

3.5.2 Elected community representative scenario:

“A social worker is contacted by a Councillor and is asked to disclose certain personal and sensitive personal data about a service user. The Councillor explains that he/she is representing the person in a

dispute with the local authority regarding the service they received from Adult Social Care, and requires the information to enable him to assist the individual with the complaint."

Please note the following a Member must:

a) represent their ward constituent
b) be able to provide evidence of consent by the constituent if so requested by the Council
c) use the information for the specified purpose
d) only share the information with other third parties, including political colleagues unless authorised by the Council and/or importantly in line with their official Council role
e) receive and transmit information securely

3.5.3 Public administrator scenario:

"A Councillor on the Family and Children's Services Committee attends a meeting regarding a family who are appealing a decision to reduce their financial support for their disabled child. The Councillor is provided with relevant personal information regarding the family". Please note the following:

a) The Council should only disclose sufficient information to assist a Member in undertaking their official role
b) the information provided by the Council cannot be used for any other purposes
c) the information must be securely maintained by the Member
d) the personal details of the case must not be shared with unauthorised "others" (including other Members) where individuals can be identified either directly or anecdotally.

Permanent written guidance will be produced to supplement all face to face training carried out under the above proposal.

4. Legal Implications

4.1 The legal implications are contained within the body of this report

5. Financial Implications

5.1 There are no financial implications as the training costs will be met from within ICT base budgets

Report Author

Ben Goward

Chief Information Officer (Interim)

ICT Shared Services