COUNCIL BUSINESS COMMITTEE

Use of Council Email Addresses for Council Business 5 November 2015

Joint Report of Chief Officers (Governance) and (Resources)

PURPOSE OF REPORT
To endorse the restriction of using only council email addresses for council business.
This report is public

RECOMMENDATIONS

1. **That the continuation of the existing policy based on best practice be endorsed, whereby members' council email addresses must be used for any council business conducted via email, rather than personal email addresses being used.**

2. **That subject to the above, it be noted that officers will be instructed, when corresponding with members by email, to use a member's council email address only.**

1 Background

1.1 All Council Members have signed up to the Members' Computer Usage Agreement Policy which includes: "Members are provided with an email address, in the form {name}@lancaster.gov.uk, for the purpose of conducting council business. Confidential council information must not be forwarded to personal email accounts (see ICT Best Practice Guide – *Reasons not to use personal email for work purposes*)." The guide is attached to this report.

1.2 It has been highlighted that some Members would like to use [or continue to use] their own personal email addresses to conduct council business, hence this report. Furthermore, ahead of Officers implementing measures to stop and/or prevent any extension or continuation of the use of personal email for council business, it makes sense to seek endorsement of good practice from this Committee.

1.3 Notwithstanding those intentions, Officers do understand that in simple convenience terms, using just one email account for both personal and work matters may seem attractive to some.

1.4 There are some major legal and practical matters that prevent such a solution being appropriate, however, and these are outlined in this report.

1.5 In the past, in exceptional circumstances, it is acknowledged that the limited use of personal email accounts has been allowed but this was only to help address extraordinarily difficult circumstances and it required additional considerations and processes to be put into place. It was not a permanent arrangement for consistent use across the Council.

2 Data Protection Act and Freedom of Information Act Considerations

2.1 The Data Protection Act lists 8 principles that require data to be:

- 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 UK without adequate protection

2.2 In addition, the Council is legally obliged to provide information when it is requested under certain Acts, such as the Data Protection Act and the Freedom of Information Act.

2.3 If all emails are processed through work systems it makes the job of management and retrieval relatively straightforward and therefore compliance is relatively straightforward and cost-effective. Where communications are sent through third party software (including personal email accounts) they would also come in scope under the Acts and so communications sent through them would need to be managed and reported accordingly. In such a situation, however, the Council would have no way of being able to do so, as it would have no knowledge or reporting capability to interrogate such third party systems / personal email accounts, and no way of controlling the associated data.

2.4 In short, by transferring data outside of the Council's network and losing the controls over managing data, the Council faces various data protection principles being breached. For normal day to day business this is considered unacceptable.

2.5 Practical differences between the different types of email accounts and their implications are outlined below, to provide more detail.

3 Differences between Personal and Council Email Addresses

3.1 The Council has a secure internal network where members and staff can use email to exchange information in relation to council business. As long as they are emailing within this network they do not need to consider all the information handling principles around security for each email they send.

3.2 The Council has no way to control or secure emails going to personal email addresses and, even if email encryption was used, then the device used to access the personal emails could have been compromised and may be forwarding all information from it to an unknown third party.

3.3 Members are issued with devices that are managed and securely maintained by the Council, so that they can conduct council business in a secure environment.

3.4 To maintain the assumed security within the internal network the use of auto-forwarding rules that send on emails to email addresses outside of the Council's secure network is not allowed.

3.5 Whenever an email is sent outside the Council network the person sending the email needs to consider the information within the email and the route that the email will be taking to reach the intended recipient.

3.6 When a private individual decides to communicate via a personal email address they are normally only communicating their own information and so can make the decision for themselves.

3.7 Whilst it is recognised that a lot of information used by the Council is open to the public, a Council member or a member of staff using email for council business can be exchanging information that may be personal to another individual, confidential council material exempt from public disclosure, or information that may cause harm to others and/or reputation/financial damage to the Council.

3.8 Furthermore, the use of an email address with 'lancaster.gov.uk' helps to give assurance as to the source of such communication and indeed to the recipient. It helps reinforce the important message that it is the Council (through a representative) with which an external party is in communication with. Even with internal communications though, the standard format of council emails helps with identification. Personal emails with, for example, very short aliases can be readily mistaken for SPAM / marketing ploys – even with filters, some staff may be in receipt of many such emails and ascertaining their true purpose and sender may not be obvious. There is therefore the risk either of emails being overlooked, or time being wasted.

3.9 In short, it is good practice to have separate personal and work email addresses, to help and to ensure that associated legal obligations are met and that the Council can work securely and efficiently. It is standard practice in organisations, to the extent that when this concept has been raised with public sector ICT and information communities, it has been met with genuine surprise as to why it would need explaining or justifying.

4 Summary of Consequences of Data Protection and Security Breaches

4.1 The Council may suffer financial loss through the mishandling of data and the Council not meeting its legal obligations, This can be in the form of direct fines from the Information Commissioner (IC), or through costs arising linked to any agreement with the IC to ensure compliance with one or more of the data protection principles.

4.2 The Council has a position of trust with the local community and businesses and this may be broken by a data loss, leading to mistrust and reputational damage.

4.3 Financial and/or physical harm may come to an individual if certain data concerning them gets into the wrong hands.

4.4 In short, data/information is a valuable commodity and systems, processes and protocols should reflect this.

5 Conclusion

5.1 Whilst needing to use different email addresses in different environments may cause a small amount of inconvenience for individuals, the risks around the use of personal email addresses for council business far outweigh the benefits.

5.2 Council business must therefore only be conducted using council email addresses, and the Committee is requested to endorse this. Officers will then be instructed to correspond with elected members by email only to a member's council email address. Any supporting operational arrangements may also be put in place, if or as necessary.

CONCLUSION OF IMPACT ASSESSMENT **(including Health & Safety, Equality & Diversity, Human Rights, Community Safety, Sustainability and Rural Proofing)** Computer usage policies aim to minimise any adverse impact, through ensuring and promoting adequate data security and appropriate working arrangements.
LEGAL IMPLICATIONS The legal implications are set out in the report.
FINANCIAL IMPLICATIONS There are no direct financial implications arising, on the basis that that the Committee endorses good practice.
OTHER RESOURCE IMPLICATIONS **Human Resources/ICT /Property/Open Spaces:** As set out in the report, where appropriate.
SECTION 151 OFFICER'S COMMENTS The s151 Officer has contributed to this joint report, in her capacity as Chief Officer (Resources).
MONITORING OFFICER'S COMMENTS The Monitoring Officer has been consulted and supports the recommendations set out in the report.

BACKGROUND PAPERS	**Contact Officer:** Chris Riley

See attached ICT Best Practice Guide – *Reasons not to use personal email for work purposes*	**Telephone:** 01524 582106 **E-mail:** cjriley@lancaster.gov.uk **Ref:**