CORPORATE GOVERNANCE AND STANDARDS COMMITTEE

29 NOVEMBER 2018

SUPPLEMENTARY INFORMATION SHEET

1

This page is intentionally left blank

CORPORATE GOVERNANCE AND STANDARDS COMMITTEE

29 NOVEMBER 2018

SUPPLEMENTARY INFORMATION

AGENDA ITEM 7 – SUMMARY OF INTERNAL AUDIT REPORTS (APRIL TO SEPTEMBER 2018)

Correction:
In the table of Ombudsman findings in paragraph 9.1 on page 95, the finding in respect of AJ-18-0002 should read "Upheld: maladministration & ***no*** injustice".

AGENDA ITEM 8 – ICT POLICIES

In order to assist councillors in their understanding of the implications of paragraph 6 of the draft Councillors' ICT Policy (Appendix 5 to the report – see page 173 of the agenda), it is proposed to include some guidance on information held in private email accounts, particularly information security considerations. A copy of this guidance, which it is suggested, should be appended to the Councillors' ICT Policy, is attached.

Official Information held in Private Email Accounts

The purpose of this document is to provide additional information for Councillors when considering the updated ICT Policy for Councillors and in particular the use of private email accounts for the official business of a public authority.

Freedom of Information Act (FOIA)

The Freedom of Information Act 2000 (FOIA) gives rights of public access to information held by public authorities.

This guidance is intended to clarify the legal status under FOIA of information relating to the business of a public authority held in private email accounts in particular, but also other media formats.

This guidance does not deal with exemptions which might be applicable to information held in private email accounts, only whether it may be held for the purposes of FOIA.

Key Facts:

- FOIA applies to official information held in private email accounts (and other media formats) when held on behalf of the public authority.
- It may be necessary to request relevant individuals to search private email accounts in particular cases.
- Adherence to good records management practice can assist in managing risks associated with the use of private email accounts for public authority business purposes.

What the FOIA says:

Section 3 sets out the two legal principles by which it is established whether information is held for the purposes of FOIA.

> **3.** (2) For the purposes of this Act, information is held by a public authority if—
>
> > (a) it is held by the authority, otherwise than on behalf of another person, or
> > (b) it is held by another person on behalf of the authority.

Under section 3(2)(a) information will be held by the public authority for the purposes of FOIA if it is held to any extent for its own purposes. Only if information is held solely on behalf of another person will the public authority not hold it for the purposes of FOIA.

Section 3(2)(b) provides that in circumstances where information is held by another person on behalf of the public authority, the information is considered to be held by the authority for the purposes of FOIA. It is this sub-section that is of relevance to information held in personal email accounts.

The Information Commissioner's Approach

The Information Commissioner states:

Information held in non-work personal email accounts (e.g. Hotmail, Yahoo and Gmail) may be subject to FOIA if it relates to the official business of the public authority.

All such information which is held by someone who has a direct, formal connection with the public authority is potentially subject to FOIA regardless of whether it is held in an official or private email account. If the information held in a private account amounts to public authority business it is very likely to be held on behalf of the public authority in accordance with section 3(2)(b).

This can apply to any public authority. For example, a Councillor may hold information relating to local authority business in his/her private email account on behalf of the local authority. The Commissioner is aware that the issue has also arisen in a central government context in relation to the use of non-work systems. There is a need to have a clear demarcation between political and departmental work. In the local government context, there is the same need to have a clear demarcation between Council business and work for individuals as their local representative.

Official information held in private email accounts must therefore have a clear demarcation between Council business and work for individuals as their local representative.

Information in private email accounts that does not relate to the business of the public authority will not be subject to FOIA but this does not mean it will not need to be reviewed to decide whether it is relevant to the request.

Situations where information legitimately requested under FOIA includes relevant information held on private email accounts will be rare. However, when a request for information is received, public authorities must consider all locations where relevant information may be held. This may include private email accounts.

The ICO recommends that, as a matter of good practice, public authorities establish procedures for dealing with such situations. These should outline the relevant factors to be taken into account in deciding whether it is necessary to ask someone to search their private email account for information which might fall within the scope of an FOI request the public authority has received. Relevant factors are likely to include:

- the focus of the request, indicated by the words used by the requester;
- the subject matter of the information which falls within the scope of the request;
- how the issues to which the request relates have been handled within the public authority;
- by whom and to whom was the information sent and in what capacity (e.g. public servant or political party member); and
- whether a private communication channel was used because no official channel was available at the time.

Where a public authority has decided that a relevant individual's personal email account may include information which falls within the scope of the request and which is not held elsewhere on the public authority's own system, it will need to ask that individual to search their account for any relevant information.

The enquiries made should be directed towards deciding whether any information which is so held was generated in the course of conducting the business of the public authority. If it was, it is likely to be within the scope of the request. It will therefore be held by the individual on behalf of the public authority for the purposes of FOIA.

> *Where members of staff or other relevant individuals have been asked to search private email accounts for requested information, or Official information held in private email accounts there should be a record of the action taken. The public authority will then be able to demonstrate, if required, that appropriate searches have been made in relation to a particular request. The Commissioner may need to see this in the event of a section 50 complaint arising from the handling of the request.*

Relevant information in other forms

Although the main emphasis of this guidance is on information held in private email accounts, public authorities should be aware that it applies to information in other forms. The definition of information under FOIA is provided at section 84 and states that *""information" … means information recorded in any form".* Therefore, official information recorded on mobile devices, including text messages on mobile phones, or in any other media, may also be considered to be held on behalf of the public authority in the circumstances outlined in this guidance. Again, this does not necessarily mean that such information will be disclosable, but, on receipt of a valid FOIA request, public authorities should consider all locations where the requested information may be found.

Concealment and deletion

> *Public authorities should also remind staff that deleting or concealing information with the intention of preventing its disclosure following receipt of a request is a criminal offence under section 77 of FOIA.*

For example, where information that is covered by a request is knowingly treated as not held because it is held in a private email account, this may count as concealment intended to prevent the disclosure of information, with the person concealing the information being liable to prosecution.

Records Management

The Lord Chancellor's Code of Practice under section 46 of FOIA stresses the importance, and benefits, of good records management. As such, public authorities are strongly advised to use their records management policies to clarify the types of information that could be considered as records relating to the public authority's business. These policies should include clear advice to staff that recorded information held by individuals, regardless of the form in which it is held, and which relates to the business of the authority, is likely to be held on behalf of the authority and so subject to FOIA.

The Cabinet Office Guidance to Departments On The Use Of Private Email) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/207131/Private_Email_guidance.pdf) says:

> *Government information must be handled in accordance with the requirements of the law, including the Official Secrets Act, Freedom Of Information Act (FoIA), Data Protection Act and Public Records Act.*

It further advises:

> *The decision about whether information was generated in the course of conducting Government business cannot always be clear cut. No single factor will determine whether information amounts to government information as opposed to for example personal or political information. It will be important to consider the relevant circumstances and in doing so, it may be helpful to bear in mind the following factors:*
>
> *a. Who are the originator and recipients of the information? This will not necessarily be determinative but if, for example, the sender and recipients are civil servants then this might suggest that the email amounts to Government business.*
> *b. In what capacity were the originator or recipients acting? For example, Ministers can act in several different capacities – as members of the Government, as constituency MPs, and as members of a political party.*
> *c. What function was the information being provided for? For example, was it to inform a substantive policy discussion or a particular decision and if so, what was the nature of that discussion or decision? Was the information being generated directly to inform or influence the development or implementation of departmental policy or the operation of the department? Should the information form part of the public record? An exchange which mentions a department's policy area (e.g. commenting, expressing views, or discussing wider political ramifications) does not necessarily amount to Government's official business. However, if it was intended that the department would use or act on the information in the course of conducting its business that may well point to the information being Government information.*

The same principles can be applied to local government.

Information Security Considerations

It is important to ensure that information transmitted between organisations is done so safely and securely. Local organisations will need to balance reputational risks, legal implications of fines (through the DPA or GDPR) which significantly raises the standards that organisations need to meet) and other consequences with the amount they intend to invest in local solutions.

Safe and secure transfer of information can be undermined by poor handling (for example information from the email may be printed off and mishandled by individuals, teams or organisations). Data Loss Prevention controls cannot be enforced when using personal emails for Council business. Securing email for safe transmission is only one small part of the process to ensure that information is handled effectively. Senior Leaders across the Council have a duty to ensure that information is sent safely and securely.

When email systems were designed, the world was a different place. The threat of cyber-attacks did not exist twenty years ago. Today it is even more important that information is exchanged securely and safely, with the risks of unlawful interception, viruses or threats because of emails with harmful attachments / links being better understood and reduced as a result.

Of course, these threats can never be totally removed and human error will always be a risk. However, by putting in place the necessary security arrangements, by

supporting staff, and ensuring that email systems are correctly configured, these threats can be significantly reduced.

The use of non-governed, non-secure (i.e. poorly configured) email accounts to exchange personal and/or sensitive information, can lead to information leakage and unauthorised sharing. The risks of loss and reputational damage to the individual or Council can be significant, particularly when it comes to privacy and harm.

General Data Protection Regulation

GDPR provides a legal requirement for the protection of personal information.
As a principle, all personal data should be encrypted (whether sent by information systems or accessed on a mobile device). The ICO provides guidance on the area of data transfers. This means ensuring that information is adequately protected from the point of transmission. This can be achieved using secure methods. This will need to include network protection through encryption (called Transport Layer Security), protecting the Domain Network Service (DNS), protecting the integrity of the actual email in transit and having governance in place to reject untrusted / spoofing emails. Rejecting untrusted emails reduces the risk of an individual inadvertently clicking malicious links and activating malware. Care needs to be taken to balance this with an approach which reduces the quarantining of legitimate correspondence.

Secure information exchange however, refers to more than just email. It is about risk management, information governance and network security. There are a number of factors to be considered when sharing information.

There are three levels of Government classification for the handling of information. This scheme operates within the framework of the Official Secrets Act (1911), the Freedom of Information Act (2000) and the Data Protection Act (1998). The classification divides data into three categories – OFFICIAL, SECRET and TOP SECRET.

For councils (and many other public sector organisations such as Health, Fire and Rescue, Community Policing as well as Charities) there is only one classification – OFFICIAL. The threat profile, information risks and attackers may differ, but the OFFICIAL level is consistent across those public sector bodies. Indeed, all personal information protected under the Data Protection Act, including health and care information, is classified at this level.

Within this, OFFICIAL-SENSITIVE is not a separate level but instead is a handling caveat for a small subset of information which is marked as OFFICIAL which requires special handling by staff. For example, a Council committee report with options for a re-organisation, a child protection file containing Police intelligence information, patient medical files and an internal fraud investigation file could all be marked as OFFICIAL-SENSITIVE. In each of these cases, the marking of ‘sensitive’ is about the handling of the data and the ‘need to know’, i.e. who is allowed to see it.

Key Principles for Councils

1. Keep personal / sensitive information in emails to the minimum necessary for the task.
If you using a remote, mobile or portable device, only carry the minimum amount of information with you. For instance, a care worker who works remote from the office and uses a tablet for client records should set the email preferences to only store a week’s worth of email on the device. This reduces the amount of information held and minimises the threat if the device is lost.

2. Only use email when there isn't an alternative.
Email is not the best medium to use for communicating personal / sensitive information. Over the years email has become pervasive. Some email systems provide flags, markers or categories. Use these to clearly identify those emails which contain personal / sensitive information. This makes it easier to manage and delete these emails as soon as possible.

3. Talk to partners, discuss and understand the flows of information to be sent by email. Regularly review and discuss agreements and decisions made.

As organisations change their methods of sharing information securely (such as in the options described in this paper) it is important to have dialogue with partner organisations to whom information is being sent to ensure they are aware and are able to test this flow of information. This should be regularly reviewed across local organisations.

4. Do not store personal / sensitive information in emails for longer than necessary
Only keep emails containing personal information for the minimum time necessary to complete the task. This is especially important for portable and mobile devices.

5. Always consider the environment you are in, when accessing personal / sensitive information.
If you are not in your office environment, be aware of your surroundings, especially if in public places, in the home of clients, on public transport etc. Can you be overlooked? Can unauthorised people see the information you are reading or what you are typing?

6. Always check with the owner of the information before forwarding it to a third party.
It is very important to "Think before you click" especially when entering email addresses and forwarding personal / sensitive information to a third party. Do you have permission to send the information? Is it yours to send? Do not forward work related emails with personal / sensitive information to personal email accounts.

7. Avoid storing and accessing personal / sensitive information on untrusted devices.
If you use your own device for work, think very carefully about what you access and store on it. You do not own that data. If the device is lost or stolen there could be real issues.

8. If you are not sure about anything relating to personal / sensitive data, seek advice.
It is better to get advice and training than make a mistake that could lead to a data breach, loss or theft.

9. Always report issues, loss or data breaches as soon as possible.
You should always report issues or suspected incidents as quickly as possible. This will always allow the most time to solve and fix problems.

10. Ensure any devices accessing personal / sensitive information are regularly updated and secure.
Always ensure devices are kept up to date with security patches and regularly scanned. Ensure all security settings are switched on. Regularly delete unnecessary personal information you have stored.

Official information held in private email accounts

The Information Commissioner further advises that in order to avoid the complications of requesting searches of private email accounts, and other private media, records management policies should make clear that information on authority-related business should be recorded on the authority's record keeping systems in so far as reasonably practicable.
(https://ico.org.uk/media/1147/official_information_held_in_private_email_accounts.pdf)

It is accepted, that in certain circumstances, it may be necessary and unavoidable to use private email for public authority business. The Information Commissioner therefore advises there should be a policy which clearly states that in such cases an authority email address must be copied in to ensure the completeness of the authority's records. In this way, records management policies will make it easier for public authorities to determine whether information is held and to locate and retrieve it in response to requests. If the information is contained within the public authority's systems it can also be subject to consistently applied retention and destruction policies.

The Councillor will be personally responsible for ensuring the appropriate management of private email accounts including the legal obligations related to the retention, disclosure and destruction of any items held in respect of public authority business.

Summary of Specific Advice for Local Councillors

Having considered the two legal principles set out in FOIA at section 3(2)(a) and (b), it may be useful to consider the position of councillors in local government because information held in relation to them can involve both these principles. This derives from the fact that elected members of a council are likely to have a number of different roles. Some will relate to their function as elected members (for example, corresponding with residents in their ward, discussing council business with fellow members in the context of voting strategy or campaigning on behalf of a political party) and some will relate to the functions of the local authority (for example, being a cabinet member and having executive responsibility for a service area, carrying out administrative functions or representing the authority, such as on a regional forum).

Information produced or received by councillors may be held on their own computers or in their own homes or offices, or it may be held on local authority premises or computer systems. However, the purpose of the information and the capacity in which it is being held is more helpful when deciding whether information is covered by FOIA.

Local authorities are public authorities for the purposes of FOIA, but individual elected members are not. Therefore, information held by councillors for their own purposes will not be covered by FOIA, but information they hold on behalf of, or as part of, the local authority will be covered (section 3(2)(b)).

Information created or received by a councillor but held on a local authority's premises or computer system will be covered if it is held by the authority on its own behalf (section 3(2)(a)). It will not be covered by FOIA if it was produced by the councillor for private or political purposes and the authority is just providing storage, office space or computing facilities (i.e. the authority is not holding the information to any extent for its own purposes).

Practical considerations

In order to comply with the requirements of FOIA, public authorities clearly need to know what information they hold for the purposes of FOIA. This means they need to be aware of information they are solely holding for another person and information that is being held on their behalf by other persons.

With regard to the former, public authorities need to know the basis on which they hold information in their possession, and with regard to the latter, what information is held on their behalf by another person and also have arrangements in place which allow them to retrieve the information in the event of a request (eg FOI or SAR) being made for it. Good records management is important in this context. Public authorities are advised to follow the guidance set out in the Lord Chancellor's Code of Practice under section 46 of FOIA. This includes, for example, a section on records that are shared with other bodies or held on their behalf by other bodies.

Recommendations:

Considering the advice provided by the Office of the Information Commissioner and the Cabinet Office guidance the Information Risk Group (chaired by the Council's Senior Information Risk Owner) and Data Protection Officer highly recommends as a part of the reviewed and new ICT policies, the use of personal email accounts for council business by either councillors or staff ceases. There are two main reasons for this recommendation:

- to eliminate the risk posed by conducting official business using non-governed and non-secure accounts;
- in order to fully comply and appropriately manage council and official information in line with FOIA and GDPR.

It is further recommended that if public authority business is unavoidably dealt with via a private email account then copies of all responses must be forwarded to the relevant official mailbox to ensure the Council has full visibility of all information as soon as possible. (Any further correspondence should be issued via the official mailbox as soon as practicable after the initial response.)

This recommendation does not prevent nor seeks to prevent Councillors from dealing with constituent enquiries or sharing information which is already in the public domain such as press releases or published documents using personal mailboxes. It does provide an appropriate balance in the management of our obligations relating to information and Councillors' ability to execute their responsibilities.

This supplementary advice and the associated policies are ultimately designed to maintain transparency in the Council's dealings with the public and enhance public trust and confidence in the Council's information management practices.

This page is intentionally left blank