Using personal emails for business purposes: The pitfalls

Doyle Clayton Solicitors **Piers Leigh-Pollitt**, **Mike Hibberd** and **Katie Mahoney** advise on consequences such as losing control of personal data and breaching the UK GDPR.

Matt Hancock's resignation won't have escaped the attention of anyone with a vague interest in the news. In addition to the revelations of his affair with his aide, Gina Coladangelo, questions were immediately raised about how the CCTV footage had been captured in the first place [see discussion on employers using surveillance and CCTV[1]]. However, a further fallout has surrounded ministers' use of personal email accounts for government activity.

While use of personal email accounts seems surprising for government business, and the authors of this article are steering clear of speculating why ministers may prefer to use personal email accounts over the course of the Covid-19 pandemic, if an employee acted similarly, there could be severe consequences for the business.

This article explores this revelation in an employment context and outlines why private mail accounts should not be used for work activity. It also covers best practices for employers to implement, both for a business's own interests and for data privacy reasons.

Government ministers using personal email accounts

The *Sunday Times* reported on 27 June 2021 that Mr Hancock faces an investigation for using a personal gmail account, rather than an official email account, to conduct government affairs during the Covid-19 pandemic. While the government's investigations will explore this under ministerial guidelines, in a normal employment context, this still gives rise to data issues.

The concern was reportedly revealed in minutes from a meeting between senior officials at the Department of Health and Social Care (DHSC) in December 2020. The minutes reportedly state that David Williams, the department's second permanent secretary, warned that Mr Hancock "only" deals with his private office "via gmail account" and "did not have a DHSC inbox".

Subsequent media reports suggest Matt Hancock is not the only one to use personal email accounts. Other DHSC ministers (such as Helen Whately, the Social Care Minister, and junior Health Minister Lord Bethell) are accused of the same. Downing Street acknowledged Lord Bethell's use of a personal email account but suggested this is within the rules.

Interestingly, the government's guidance on private emails does not contain an absolute ban on using personal email accounts, but states "it is expected that government business should be recorded on government record systems".[2] It states that those conducting government business "should ensure the relevant information is accessible e.g. by copying it to a government email address".

> ICO is concerned that information within private email accounts or messaging services is not properly secured from a data protection perspective.

Information Commissioner's Office investigation?

In response to the ongoing revelations, the Information Commissioner's Office (ICO) is now investigating the DHSC's use of personal email accounts. The ICO served information notices on the DHSC (along with unspecified others) to try to establish if private correspondence channels have been used, and if so, whether this use breached freedom of information or data protection laws.

According to the Information Commissioner, Elizabeth Denham's, blog on 6 July 2021, the ICO is concerned that information within private email accounts or messaging services is not properly secured from a data protection perspective and could be forgotten, overlooked, autodeleted or otherwise not available when a freedom of information request is made.[3]

The ICO will not comment further until its investigations conclude and it publishes its findings.

Court challenge

In addition to the ICO's investigations, the campaign group Good Law Project has launched a legal challenge against the government, arguing current official guidance on use of personal communication channels leaves an "accountability gap".

According to reports, the Good Law Project has sent a pre-action notice to various government departments around alleged use of private messaging accounts. We will need to monitor ongoing developments, including whether a judicial review is launched.

The risks for businesses

Businesses need clear expectations on communication channels their staff can use. Using personal email accounts carries significant risks. These include:

Loss of audit trails and difficulties retrieving data for litigation: The first obvious risk is that a business loses audit trails if employees use personal mailboxes, even if this is with the employer's knowledge. An employer cannot quickly search for all the information needed to meet audit requirements, respond to customer queries, nor quickly retrieve evidence that it is fulfilling its legal obligations, if investigated. For regulated organisations, this

also carries regulatory risks if they cannot provide evidence of compliance to the regulator when asked.

If any litigation is instigated against the employer, information on personal accounts is harder to retrieve (and individuals may argue their own mailboxes are private).

Loss of control of personal data / UK GDPR breaches: By using personal accounts, employers will lose control of data and it will be hard to forensically review the data in personal mailboxes.

Such actions also risk breaching the UK General Data Protection Regulation (UK GDPR) (and the obligation to inform data subjects (such as customers and/or clients) how their data will be used) if the individual is not informed their data might be shared to a private email account. Similarly, colleagues are unlikely to have been made aware their details could be sent to a colleague's personal email account.

Employers must also have appropriate security safeguards in place to protect personal data, including protection against unauthorised or unlawful processing.[4] Permitting use of personal email addresses for work activity is likely to fall foul of this safeguard.

Using personal email addresses could also amount to unauthorised or unlawful processing, since the data controller will no longer be the employer but the individual employee. The employee is very unlikely to have put in place any data protection controls before or during any processing activity. If the individual is located overseas, there are further potential risks if appropriate safeguards are not used when transferring the data overseas.

Problems for Data Subject Access Requests: Using personal email addresses for work purposes also makes it harder for organisations to comply with Data Subject Access Requests (DSARs) because they will not know what data is held, where it has gone and how long it is retained. It is arguable that personal mailboxes could fall outside the scope of a DSAR if the business is not the controller of that data. Similarly, it is possible that personal accounts (depending on the facts) fall outside a "reasonable and proportionate search," and so an organisation would not have to search them when responding to a DSAR (as found in previous case law). However, if a requester finds their information has been sent to personal email accounts without their knowledge and they have not been informed of this, the ICO will likely follow up on this and find a potential data breach.

The ICO's detailed DSAR guidance[5] also raises the possibility that personal email accounts do, sometimes, fall inside the scope of a DSAR. The guidance states: "A policy should restrict staff's permission to hold information about customers, contacts or other employees on their own devices, in private email accounts or on private instant messaging applications."

"Staff accessing systems remotely (for example via a secure website) should not hold personal data on equipment the employer does not control."

"If staff may hold personal data on their own devices, they might be processing that data on the employer's behalf, so this could be within a DSAR's scope. This depends on the purpose for which the employer holds the information, and its context."

"The ICO does not expect employers to instruct staff to search their private emails, personal devices or private instant messaging applications in response to a DSAR, unless the employer has a good reason to believe they are holding relevant personal data."

The ICO's suggestion that such accounts could, depending on the circumstances, fall within a DSAR response, highlights a further risk of permitting use of personal accounts.

Data security risks: Storing personal data originally obtained by the employer (for example on customers and clients) on personal email accounts also increases the exposure to hackers and security breaches if the personal email account is hacked.

Commercially sensitive information falling into the wrong hands: Businesses holding commercially sensitive information will want to ensure their sensitive information does not fall into the wrong hands, such as those of a competitor if an employee has the information on a personal device and leaves the organisation.

The risks for individuals

Data protection risks: Rogue employees considering removing data from personal accounts should be aware it is a criminal offence under the Data Protection Act 2018 for individuals to, knowingly or recklessly, "unlawfully obtain personal data".[6] This sometimes happens when departing employees take customer information with them to use at a new organisation. The ICO has acted in the past against such individuals, leaving them with a fine and criminal record. Its enforcement actions are published online too, which clearly has implications for the employee in future job searches.

Litigation risks: More often than not, communications from personal accounts form part of the evidence in employment-related litigation, particularly in the High Court. Although many employees think that communications sent on personal devices and personal accounts are unlikely ever to be scrutinised by the court, they have actually featured in some of the biggest employment-related cases in the High Court in the last two years.

Litigation over a group of employees leaving an organisation regularly involves employees using their personal email accounts to email each other and arrange the unlawful move. The court regularly requires the employees to provide their personal devices to forensic IT consultants to search for certain communications. In many cases, even where employees think they have permanently deleted communications from their personal email accounts, the forensic IT specialists are able to recover these communications. It is often these communications, which come out as part of the disclosure process, that demonstrate the extent of the skulduggery which has been at play.

Best practices for employers

An absolute prohibition on personal email accounts for business clearly limits the above risks. Justifying any occasional use will depend on the facts. For start-up organisations, corporate mailboxes might not be the first thing on the entrepreneur's mind, but they should consider them promptly.

To mitigate the risks, employers should:

1. Have a clear data protection policy

outlining what staff may do with personal data. This should include mandating use of official business email accounts and not transferring data to personal accounts.
2. Train staff periodically on data protection and review and update internal policies regularly.
3. Ensure staff know how to identify and raise concerns about any data breaches.
4. Explain to staff how breaches of the data policies will be treated, for example potentially leading to disciplinary proceedings up to and including dismissal.
5. Implement technical safeguards – for example alerts which can be sent if emails are forwarded from corporate to personal accounts.

AUTHORS

Piers Leigh-Pollitt is a Partner, Mike Hibberd an Associate and Katie Mahoney a Legal Director at Doyle Clayton Solicitors.
Emails:
PLeigh-Pollitt@doyleclayton.co.uk
KMahoney@doyleclayton.co.uk
MHibberd@doyleclayton.co.uk

www.doyleclayton.co.uk

REFERENCES

1 www.doyleclayton.co.uk/resources/news/covert-cctv-recordings-at-work/
2 assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/207131/Private_Email_guidance.pdf
3 ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/07/ico-launches-investigation-into-the-use-of-private-correspondence-channels/
4 UK GDPR Article 5(1)(f)
5 ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/
6 DP Act 2018 s. 170(1)(a)