Browne Jacobson

Avoiding the pitfalls of WhatsApp

The use of social media platforms and applications can have overwhelmingly positive benefits for public bodies. However, regulatory action recently taken by the Information Commissioner, has highlighted various pitfalls that public bodies should seek to avoid if allowing staff to use social media as a communication tool.

25 August 2022

The use of social media platforms and applications can have overwhelmingly positive benefits for public bodies. These technologies not only provide an effective means by which public bodies can communicate with the public, but also provide a platform for staff to exchange information, organise and make arrangements.

However, regulatory action recently taken by the Information Commissioner, disciplinary cases brought against staff and professionals who misuse social media, and judicial review challenges to central government have highlighted the various pitfalls that public bodies should seek to avoid if allowing staff to use social media as a communication tool.

First, the Information Commissioner has recently released the report "Behind the screens - maintaining government transparency and data security in the age of messaging apps" following a year-long investigation into the use of messaging apps by Ministers and officials at the Department of Health and Social Care (DHSC) during the pandemic. The investigation found that a lack of clear controls and a rapid increase in the use of messaging apps had the potential to lead to important information being lost or insecurely handled. In particular, the Information Commissioner was of the opinion that:

- DHSC did not have appropriate organisational or technical controls in place to ensure effective security and risk management of private correspondence channels being used.
- DHSC's policies and procedures were inconsistent with Cabinet Office policy on the use of private email (June 2013) and had some significant gaps based on how key individuals were working in practice.
- The use of such channels in this way also presented risks to the confidentiality, integrity and accessibility of the data exchanged.

Second, it is important to remember that the use of messaging apps does not remove information from the reach of the Freedom of Information Act 2000. The Information Commissioner has separately set out five key recommendations for public bodies to keep in mind when handling freedom of information (FoI) requests that cover such communications:

- Make sure staff, relevant public officials and elected representatives understand how they can securely access official IT systems and equipment. This should minimise the need to use private correspondence channels.
- Train staff to recognise which communications relate to official business and which relate to non-official information across all channels. In the context of local government, there should be a way of distinguishing between official business and an elected official's work on behalf of their constituents.
- Review and communicate records management policies. Staff should be regularly informed of what they need to do to ensure information related to public authority business is transferred to official systems as soon as possible.
- When handling FoI requests, public authorities should consider whether communications held on private correspondence channels, such as WhatsApp, may be relevant to the request.
- Ensure staff correctly adhere to the relevant policies and procedures and regularly review them to ensure staff knowledge remains up to date. Remember, erasing, destroying or concealing information with the intention of preventing disclosure is received as a criminal offence.

Third, there have been two high profile judicial review challenges in which it has been argued that the use of self-destructing messages on insecure platforms is of itself unlawful and undemocratic. We understand that judgment in those proceedings is currently reserved and we recommend that public bodies scrutinise closely any guidance given by the courts about the use of such apps in due course.

Fourth, it is important that public bodies have comprehensive social media policies in place that allow staff to understand what is permitted by the organisation, and the circumstances in which any improper use of social media (whether in private or professional life) may lead to disciplinary or regulatory action being taken. There have now been several high profile cases over the last few years whereby action has been taken against police officers, contractors of the Home Office and doctors for variously sharing information that was regarded as offensive (amongst other things). Staff should be reminded that the use of closed forums are never truly private, and information shared with colleagues using WhatsApp and other social media apps has the potential to harm the reputation of an organisation and staff, and undermine public confidence in the organisation or a profession generally.

Browne Jacobson has a team of experts that can assist public bodies in updating their policies, responding to FoI requests/DSARs and regulatory action, and taking action against staff when social media is misused. Please contact us if you have any questions about this article or require assistance in dealing with these issues.

The same position applies to data subject access requests (DSARs).

Contact

Matthew Alderton

Partner

matthew.alderton@brownejacobson.com

+44 (0)330 045 2747

Related expertise

Services

Criminal compliance and regulatory

Data protection and privacy

Digital and data

Freedom of information

Information law

Regulatory