Spotlight on…… Governor email addresses

We still come across some schools where Governors are using their own email address rather than a school email. Or, they have a school email, but they auto forward the emails to their personal email (which is as bad as not having a school account in the first place).

Governors may be receiving information about a disciplinary matter; parent complaints; or financial information, and even if the data is not personal, it could still be confidential business information that would not be included in the final minutes or available to the general public. Whilst the minutes are available to the general public, generally the supporting information is not. Here are a few risks that exist if governors are not using a school email address.

- You have no control over who can access the governor emails at home (we've seen governor emails that are along the lines of "Mr&MrsSmith@hotmail.com" which suggests it was not used solely by the Governor themselves!)
- You also have no control over the kind of security they have on their home systems – do they have anti-malware and anti-virus set up for example? If not, the data is not secure and is certainly not as secure as the platform you will have provided with the school account. Your Security Measures document details how you keep your data secure – much of it would not apply once the email has left your system.
- What if they get a new computer – do they wipe the hard drive in line with industry standards to ensure any data held on there cannot be not retrieved prior to taking it to the refuse centre? Or do they donate it to a family member, or sell it online? In any of these scenarios, data (even if it has been "deleted") can be retrieved.
- If a subject access request was made and the Governor held any personal data relating to that particular data subject (e.g. a member of staff), they would need to retrieve that data and send it.
- If a governor resigned, how would ensure all the data relating to the school (whether personal or business confidential) was destroyed / deleted appropriately?
- Governors tend to get involved in complaints; disciplinary matters etc all of which can be highly sensitive – if it were your personal information, would you be happy that it had been forwarded to someone's home email account where there are no controls in place to secure it, rather than being kept in the school where you have policies and procedures that dictate how data is kept secure, both organisationally and technically?
- A few years ago, a senior member of staff at ECC had auto-forwarded their emails to their home email address (against ECC policy). Their home laptop was stolen and (unlike their ECC issued one) it was not encrypted (we tend not to encrypt our personal devices). Because of the nature of data held on their emails, we had to report this to the ICO. We were spared a fine, but the ICO did audit ECC as a result. One of the actions we took pretty quickly was to put a technical solution in place to prevent any member of staff auto-forwarding their emails to a non ECC email address.

We have also been asked about printing off this information and storing it in the governor's home. Previously some schools printed all the information and kept them in school in governor folders, which would not be removed from school, but due to Covid this practice is not possible at the moment. Ideally, if the governor is able to access their school account, information would not need to be printed off, but where this is a requirement, in the current circumstances, a reassurance in writing that information will be stored securely on home premises, and then either returned or shredded when no longer required would be acceptable.

Zoom is a US company that stores data in the US. This is particularly problematic at the moment due to the Privacy Shield collapsing in July.

We are happy for Zoom to be used for meetings as the only personal data shared and stored in the US are emails – these are not particularly sensitive so low risk. There is a Zoom DPIA in the library that covers this purpose.

What we cannot approve though, is recording Zoom meetings. The recordings would be stored in the US and currently there is no mechanism in place that would make storing that amount of personal data safe or legal. Your school has MS Teams and that will be a much safer way of recording meetings if you wish to do that.