Ransomware/phishing/data security - Advice given to staff:

- No organisation is invulnerable and we cannot afford to be complacent.
  The DfE has highlighted a wave of attempts to extort money from independent schools through ransomware.
- The School has three main measures in place:
  - An enterprise level Firewall that prevents most malware and viruses from reaching our network.
  - Sophos antivirus software on our workstations to capture threats locally.
  - A programme of regular software updates and security patches (these have ordinarily been undertaken over holidays and weekends, but we are now applying these more immediately).
- Phishing. In view that ransomware is spread through email phishing attacks, the most important and effective protection is staff awareness of this:
  - Always check the authenticity of a sender by checking the sender's email address. If an email says it is from Joe Matthews, for example, and contains links or downloads ('click bait'), check the email address and if it is not an '*..@cityoflondonschool.org.uk*' address, delete the email or contact him first if you remain suspicious. You can check an email address either by clicking, or hovering over the sender's address, eg: ***From**: Joe Matthews*).
  - Even if the sender's email address appears authentic, be suspicious if it contains links or downloads.
  - Similarly, be alert to suspicious suffixes, eg: *bt.info* (instead of *bt.com*) or *..@mail.paypal.com* or *.info* etc (instead of *..@paypal.com*).
  - Phishing scams attempt to concentrate on and masquerade as senior roles in an organisation. So, an email with links/downloads from the Head, Bursar or Finance Office, for example, should be scrutinised before following the links. Again, check the actual sender email address before actioning the email and contact the sender if in doubt.
  - Do not follow links, or download files without being sure that they are genuine.
  - If in doubt, ask: the sender, if they are available; or the IT Dept.
- Additional measures:
  - The School is adopting Microsoft Windows 10 in view of its enhanced security features. You will notice this in the Staff Quiet Room and staff Dept Common Rooms first.
  - We are also bringing forward our research into adopting Microsoft Office 365 for the same reason and enhanced resilience.
  - We have started a programme of recalling School-issued laptops in order to upgrade them to the latest security systems.
- At home: back up your computer and important files regularly.
- Devices: ensure you install iOS/Android updates regularly.
- Further to Sarah's comment this morning, I would like to highlight the huge effort of our IT Team and Joe Matthews in particular. Many of the measures are put in place during weekends to avoid disruption to our systems. Our Team are also a very strong security measure for the School in their own right.
  - In view that some of the anti-ransomware patches/upgrades are quite major ones, we need to install these during working hours to ensure that we have technical support from the suppliers (not available out-of-hours). This may unfortunately mean a higher level of disruption than we would like, for which we apologise in advance. We shall balance this with the risk of a successful attack.
  - In view of the heightened level of threat, please make sure that you read Joe's, or IT Department emails, and take the appropriate action.