Data Protection – 12 important points

1. **Think Data Protection: be vigilant and aware of what Personal Data is** and what data you process. If a person's name and one other piece of information about that person is available and identifies them, it's personal data. Medical and religious data about someone is of a higher class of personal data and needs very strict access control.

2. **Have a strong and unique password for school use** – minimum 8 Characters with at least one capital, one number and one special character (£, $, !, #, @, etc). Use the 3 short word methodology – eg Spain Sun Sand could be "$pa1nsunSand!" Do not share your password.

3. **Do not share Personal Data unless necessary and appropriately controlled** and through formal agreements, including on-line. Eg if wanting to use an online service that requires the provider to have children's names, DoB and Gender, please don't simply provide it – check with me about contracts, data sharing agreements, etc.

4. **Protect and securely dispose of/destroy Personal Data** – secure paper disposal boxes in all staff Common rooms and other areas around the site. If in doubt, ask Lisa Weller. Don't keep unnecessary emails longer than necessary - delete.

5. **If working off-site and accessing school data** – keep it within the confines of your OneDrive, ClassNotebook, etc.

6. **If prompted to approve an off-site Log-on via the MFA/Authenticator App** – don't simply approve the request without knowing it was an action **by you** that prompted the approval process. If you're not sure, don't approve it – it could be a malicious attempt to access your account from afar.

7. **Be aware of who you are sending emails to and how**. If sending to many external email addresses, put the email addresses in the Blind CC line (so they don't see each other's email address). Check who the mail is going to before pressing send (eg staff have [STAFF], pupils have [PUPIL] after their name). Outlook warns if an email is going to external addresses. Use iSAMS email facility if appropriate – it's personalised and ensures emails are individual.

8. **Think about volume of data and control of your data** – refrain from replying to all or using wide distribution lists. Share a file/folder as opposed to attaching it to an email – this allows you to retain control and withdraw access immediately if you need to (also saves many copies of the same [large] file in many mailboxes being backed up). This is not available to send to external users at present.

9. **Judicious use of personal opinion within emails** – **use the phone/speak on Teams**! A Subject Access Request (SAR) exposes all! If you would not be happy for your comments to fall into the public domain or to the person you are referring to, speak, don't type!

10. **Don't use USB sticks or allow visitors to use USB sticks on our network/equipment** without prior approval – these are a really good route for viruses and malware to be uploaded. Use your Laptop/OneDrive account or ask visitors email their material to you or bring their own device to connect to a projector (NOT our wired network).

11. **Segregate your personal life from your professional life** – don't use school email for personal use and vice versa. Have a personal email address for personal use (with a different password!).

12. **If you commit a data breach or your account is attacked** – own up straight away so we can take appropriate action quickly. Speak to Simon Drew or any member of the SLT immediately (including out of hours).

Simon Drew 1 September 2021