Data Protection & GDPR - *Essential practices in your school*

DO

- ✓ Save electronic files to your school network drives so that they are backed up and kept safe
- ✓ When transferring personal data via email, do so using secure mail methods or password protected attachments. Always share the password via separate communication
- ✓ When sharing electronic personal data internally with colleagues, save the data to a school network drive and share a link to it with your colleagues
- ✓ Only share personal data with colleagues who have a legitimate reason to view it
- ✓ Use secure shredding when disposing of personal data or confidential information
- ✓ Contact BWT central team when procuring new systems involving the storage, use or sharing or personal data. A Data Protection Impact Assessment will be required
- ✓ Ensure that BWT Privacy Notices for parents and students are displayed in school reception areas
- ✓ Ensure that BWT Privacy Notices for staff are displayed in an appropriate and accessible space
- ✓ Keep all personal information in accordance with the "Information and Records Management Society Toolkit for Schools"
- ✓ Use school issued encrypted memory sticks when it is essential that personal data is stored or transported via such a method. Try to find an alternative method first!
- ✓ Ensure consent for the use of student photos and videos is obtained using the Trust issued template. No other versions should be used
- ✓ Lock your screen and devices when leaving them unattended
- ✓ Store files on school networks in drives allocated by your school IT teams/providers
- ✓ Ensure that all paper files containing personal data are secured in locked cabinets in secure spaces
- ✓ Use number coded key safes to store keys for access to restricted areas such as HR files, archive rooms etc.
- ✓ Ensure that staff IT passwords are changed every 90 days
- ✓ Familiarise yourself with the Trust's Data Protection Policy and associated procedures
- ✓ Keep your desk clear of personal or sensitive data
- ✓ Share the Trust's Privacy Notice for staff with job applicants so they know how we will be using the data we are gathering
- ✓ Use secure remote connections to school networks when working away from the school
- ✓ Report all data breaches immediately!

Principals and Leaders:

- ✓ Make sure that all key staff are aware of all new procedures relating to data protection and GDPR including their roles in discharging the procedures set out
- ✓ Encourage all colleagues to discuss and report concerns over data security, including observed practice, system fragility or inaccurate records. We need to welcome this and respond appropriately.
- ✓ Regularly review school systems and processes to identify new or obsolete practice, software or systems. Update the school's 'data mapping' list accordingly, working with Trust central team as required.

DON'T

- × Do not store electronic files only onto desktop computers, laptops, external hard drives etc.
- × Do not include personal data in the main body of any emails
- × Never leave personal data or confidential information unsecure – always lock it away
- × Never leave shredding bags awaiting disposal anywhere other than in a locked, secure cabinet, even temporarily
- × Do not open links or attachments of suspicious emails
- × Never use a non-encrypted device, including memory sticks, for storing and transporting data. Only use school-issued encrypted devices.
- × Don't assume that previous consent, or a lack of negative consent, is suitable permission to use a photograph or video
- × Do not leave keys to filing cabinets and archive stores accessible to anyone other than staff who have a legitimate reason to access the information
- × Do not share your username and/or passwords with anyone!
- × Do not log on to public Wi-Fi whilst working on or with personal data
- × Do not work in public spaces where other people could see or overhear personal data
- × Do not collect any personal information or data that you don't legitimately need (by law or to fulfil our statutory functions), or have consent for
- × Don't email or contact anybody, including parents, with information relating to marketing or promotional activities, including fundraising events. General school news is ok to share
- × Do not display medical records so that it can be viewed or accessed publically. Limit access to people that need to know
- × Do not leave laptops, phones, personal data or sensitive information in cars when unattended
- × Do not send data to personal email addresses to work on at home
- × Do not print personal data unless it is essential to do so. Try to work digitally as much as possible and avoid creating duplicate records
- × Do not use 'all staff' email lists to share personal data about students or colleagues

AMBITION FOR ALL › HIGH EXPECTATIONS › EXCELLENT TEACHING & SUPPORT › WORKING TOGETHER › CONTRIBUTE TO SOCIETY

If you need further clarification on any aspect of GDPR as it applies to your school or role, please contact the central team on 01536 397000 or email enquiries@brookewestontrust.org