GDPR – Key Issues for Staff

1. Data is not to be shared without following the proper procedures, even with trusted third parties such as social care and the police. *This includes people within the family, their consent must be recorded to share with an extended family member. Be particularly careful before releasing personal information by telephone.*
2. Passwords will be kept securely and not accessible to third parties
3. Passwords will comply with the School requirements for complexity
4. Passwords will not be shared
5. Automated log on processes to store passwords will not be used
6. Computers will be locked if they are unattended or auto lock to maintain security
7. Confidential or restricted data will not be left out if the office is unoccupied or left on the desk if others can access the information. This applies to hard copy and removable storage, e.g. USB memory sticks. Locked offices, cupboards and drawers are safe places to secure data, subject to the policy.
8. At the end of the day the computer must be fully shut down and log out procedures followed. Hard copy data must be securely stored and locked away.
9. Downloading new software from the internet must only be done by prior approval
10. Confidential discussion will not take place in front of unauthorised individuals
11. Sensitive information should be at least password protected before sending by email, and any password conveyed separately
12. Records and data in any form that are taken off site must be secured at all times. Leaving paper files or digital media unattended is not acceptable.
13. Make sure that if you are going to remove hard copy or digital information to work on away from school that you have authority to do this, and that where you do this is secure and safeguards are in place.
14. If out of school overnight the records and data must be stored securely. Leaving records or data in a locked car is not acceptable.
15. Mobile phones, laptops and tablets must be encrypted.
16. No memory sticks are to be used to store/share data.

17. Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the subject and the legitimacy of the request.
18. If you receive a request for personal information about another employee, you should forward this to the Business Manager, who will deal with such requests.
19. Do not access another employee's records without authority as this will be treated as gross misconduct and it is a criminal offence.
20. Do not write down opinions – by email or hard copy – about a person that you would not feel comfortable saying to their face. Record facts not opinions.
21. Treat everyone's data in the same way you would like others to treat yours!

Unauthorised or unlawful sharing of data can have serious consequences, for the data subject whose rights have been breached, the school as data controller and also for the individual who breached the GDPR. Unauthorised sharing can lead to individuals being placed at risk, particularly vulnerable children. The school could face intervention and or fines. Depending on the type of data breach the individual could face disciplinary proceedings, up to dismissal and in more extreme cases even prosecution. Most data breaches are the result of unintentional human error, but the impact of the consequences must never be ignored.

If you have any questions or concerns about GDPR please contact Lindsay Pilkington on lpilkington@dale.derby.sch.uk. Our Data Protection Officer is John Walker, who can be contacted on john@jawalker.co.uk.