Data Protection Guidance for Staff

Personal data: any information relating to an identifiable living person, e.g. name, contact details, ID numbers, attendance and assessment information, financial information.

Sensitive personal data: includes information that reveals someone's ethnic origin, political opinions, religion, sexuality or health. In our school, it also means safeguarding information, and whether a child is looked-after, has SEN, or is eligible for free school meals.

The personal data we are responsible for could include that of pupils (past, present and potential), parents and carers, staff, volunteers, visitors, governors, specialist support providers and other visiting professionals.

Paper Records

1. Keep paper records containing the personal data of students or staff secure at all times, in the classroom, around school, during transit and at home.

2. Do not leave paper records sensitive information unattended; where possible store it in lockable drawers/cupboards.

3. All paper based school trip information, medical advice contact addresses, allergies etc. must be returned to the school at the end of the trip for secure filing or shredding.

4. Keep a clean desk, don't leave sensitive information on view for students / other staff to read.

5. Collect printing that contains personal data immediately - Do not use student to collect sensitive information from printers / copiers.

6. Dispose carefully of any paperwork that contains personal – use shredders / secure bins.

Devices & Applications

7. Ensure all school devices are kept secure at all times, in the classroom, around school, during transit and at home.

8. Ensure all devices are logged off or locked when they are left unattended.

9. If you are using a mobile device (phone) to access work email or network resources, ensure that the device is password protected and notifications are set so that the content of emails is not displayed on lock screens.

10. Only use school devices to take and record student images. Ensure you have checked consent records before doing this.

11. Do not use personal devices to access, view or store school-related personal data.

12. All external USB Drives used for school purposes must be encrypted.

13. Do not acquire or use applications, software or websites requiring information on pupils/staff data without prior authorisation by the school.

14. When working with sensitive data, do not position screens where they can be easily read by other people.

Wifi, Access & Downloading

15. Do not log on to public Wi-Fi networks or use public computers whilst working with school-related personal data.

16. Access data remotely, instead of taking it off-site, using secure systems approved by the ICT Support team.

17. Do not save or download school-related data onto personal devices unless first authorised by the school.

18. Ensure that any downloaded personal data stored on a shared network drive or the cloud is password protected and permanently deleted when is no longer required.

Passwords

19. Ensure all passwords are kept secure and meet the complexity requirements when they are changed or created. Passwords must be at least 8 characters long and contain characters from three of the following four categories:

    1. *Uppercase characters of European languages*
    2. *Lowercase characters of European languages*
    3. *Base 10 digits (0 through 9)*
    4. *Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/*

- Do not share your passwords with anyone or write them down.
- Do not save passwords in web browsers if offered to do so.

E-mails

- Email accounts issued by the school are not private property and form part of the schools administrative records. The content of emails may be disclosed to individual or outside agencies, as required by the Data Protection Act 2018.

- Do not use personal (non-school provided) email accounts to conduct school business. A school email account should be used for school business and not for personal correspondence or other purposes.

- Do not open any email attachments sent by unrecognised senders.

- Do not send by email any material that is viewed as highly confidential or contains personal data, unless is encrypted/password protected. In such cases the encryption key/password must be communicated by other means (in person or over the phone).
- Ensure that emails are being sent to the intended recipient by double checking their email address before sending.

- Use the 'bcc' function when you're emailing a group to avoid sharing email addresses with everyone else in the group, e.g. parents or volunteers.

Displaying / Presenting Data

20. Keep personal data anonymous if possible, for example, if you're emailing a colleague about accommodating a pupil's religion, or about managing a pupil's medical condition, don't name the child if you don't need to.

- Be mindful what personal/sensitive data may be on display in class when visitors, agencies and parents are accessing rooms.

- Think before you display personal information on the wall in classrooms, corridors or other spaces that may be accessed by parents or visitors. If you may need consent from the parent or pupil or if there might be a safeguarding risk in displaying it. Minimise to what is necessary.

Verbal Disclosure

21. Be mindful of the spaces that you have sensitive conversations in. It is not always possible to hold private discussions, or telephone calls, but if the issue is particularly sensitive, think about who may overhear.
22. Avoid discussions involving sensitive personal data in open areas such as the school reception.
23. When visitors are present in school (especially parents) ensure that other staff are aware of their presence – to prevent accidental verbal disclosure of personal data
24. Do not discuss personal information relating to pupils, parents or work colleagues with friends or associates outside of school. There is an expectation that personal data the school is responsible for is held confidentially and should be treated as such when you are not in work.

Reminders

- Remember that data protection laws DO NOT stop you from reporting safeguarding concerns. You must still report to the relevant people where you're concerned about a child. You do not need anyone's consent to do this.

- If you have to share highly personal or confidential information, do so in person, over the phone or via a secure managed file transfer.

- Read and understand all of the school's policies on data protection.

- Only keep data for as long as is needed. If you are not sure how long to keep data for, check the school retention policy.

- Speak to the DPO / Headteacher if:
    - You have any concerns at all about keeping personal data safe
    - You're introducing a new process or policy that involves using personal data
    - Anyone asks you to see the data that we have about them. This is called a 'subject access request', and the person will be entitled to this information

- Contact the DPO / Headteacher immediately if you think personal data has been lost, stolen or wrongly disclosed.

STAFF NAME: _____

SIGNATURE: _____

DATE: