Data Protection Guidance for Staff, Volunteers and Governors

This document outlines the responsibilities that all staff (substantive staff / supply staff / training students / volunteer) have for protecting information. It is not intended to replace the school's Data Protection Policy, but instead explain some of the key concepts, working practices and behaviours that staff should understand and demonstrate when working with personal data.

Personal data: This is any information which allows a person to be identified, e.g. name, contact details, ID numbers, attendance and assessment information, financial information, or biometric information (fingerprint recognition technology).

Sensitive personal data ("special categories data"): This includes more sensitive information, it may reveal someone's ethnic origin, political opinions, religion, sexuality or health status. In our school, it also means safeguarding information, whether a pupil is looked-after, has SEND, or is eligible for free school meals.

The personal and sensitive personal data we use in school, could include information relating to pupils (past, present and potential), parents and carers, staff (current, former, individuals involved in recruitment processes), volunteers, visitors, governors, specialist support providers and other visiting professionals.

Data Breaches: A data breach occurs when personal data is compromised or used in a manner that has not been agreed (or is lawful). It can include any of the following:

Loss of personal data

- Pupils files misplaced and data not available when needed
- USB memory sticks lost outside school
- Ipad or tablet devices removed from school

Inappropriate sharing of information

- Letters sent to wrong parent
- Emails sent to wrong person
- Information used in online systems without prior approval

Unauthorised access to information

- Pupil information taken from offices/classrooms
- Phishing attacks on email systems
- IT security compromised – children or other staff able to read or access systems in school (or at home)

Data Protection Officer

The school has a Data Protection Officer (DPO) who can help and advise on any issue relating to the protection of personal data in school.

Email the Data Protection Officer: DPO@services4schools.org.uk

Paper Records

- Keep paper records containing the personal data of pupils or staff secure at all times, in the classroom, around school, during transit and at home.
- Do not leave paper records sensitive information unattended; where possible store in lockable drawers/cupboards.
- Do not leave files or records containing personal data in cars overnight, or for long periods of time.
- All paper-based school trip information, medical advice contact addresses, allergies etc. must be returned to the school at the end of the visit/trip for secure filing or shredding.
- Keep a clean desk, don't leave sensitive information on view for pupils or other staff to read.
- Collect printing that contains personal data immediately - Do not use pupils to collect sensitive information from printers / copiers.
- Carefully dispose of any paperwork that contains personal data– use shredders or secure bins/bags.

Devices & Applications

- Ensure school devices you are responsible for are kept secure at all times, in the classroom, around school, during transit and at home.
- Ensure all devices are logged off or locked when they are left unattended (hold down the Windows key and L to quickly lock your session)
- If you are permitted to use a mobile device (phone/tablet) 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.
- Only use school devices to take and record pupil images (Ipads/Cameras). Ensure you have checked consent records before doing this.
- Do not use personal devices to access, view or store school-related personal data unless this has been authorised.
- Do not use removeable storage devices. These include external USB Drives, or portable hard-drives.
- Do not use or promote online applications, software or websites that require you to provide information on pupils/staff data, without prior authorisation by the school.
- When working with sensitive data, do not position screens where they can be easily read by other people.

Wifi, Access & Downloading

- Do not log on to public Wi-Fi networks or use public computers whilst working with school-related personal data.
- Access data remotely, using secure systems approved by the school's ICT support. Do not take physical copies of personal data off-site unless this has been authorised.
- Do not save or download school-related data onto personal devices unless first authorised by the school.
- 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

- 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 enter usernames and passwords in links from emails, unless this is part of a "forgot password" process you have initiated.
- 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 school administrative records. The content of emails may be disclosed to individual or outside agencies, in accordance with the rights individuals have under 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 sensitive personal data, unless is encrypted/password protected. If you are unsure how to send information securely, check first with your IT support.
- 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 of recipients to avoid displaying email addresses with everyone else in the group, e.g. parents or volunteers.
- 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.
- Avoid retaining emails for long periods. If you need to keep the information sent in an email or attachment, download the content, or move to a saved emails folder to help reduce the amount of personal data being stored.

Displaying / Presenting Data

- Be aware of the consent preferences parents/carers have expressed, especially with regards to the use of photographs and images.
- It is OK to display work or images illustrating success in and around school, but be mindful of personal/sensitive data that may be on display in reception areas, corridors or other spaces accessed by parents/carers or visitors. Consider any safeguarding risks relating to individuals and minimise the information to what is necessary.
- Before you publish or display personal data outside of school (online or physical displays) you must seek written parental consent.

- If assessment or performance data is displayed on walls, ensure that sensitive characteristics are not displayed or labelled to identify individuals (SEND, LAC, etc.)

Verbal Disclosure

- Be mindful of the spaces that you have sensitive conversations in. It is not always possible to hold discussions, or telephone calls in private, but if the issue is particularly sensitive, think about who may overhear.
- Avoid discussions involving sensitive personal data in open areas such as the school reception.
- 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
- Don't leave personal data in voicemail or phone messages.
- 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.

Additional 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.
- Read and understand all of the school's policies on data protection
- Individuals (employees, pupils, parents etc.) have a right to access copies of their own personal information that is being used by the school. This is called a 'subject access request'. Any requests for information should be reported to the Data Protection Officer
- Parents/Carers may also be entitled to access pupil information under other legislation, please seek advice from Data Protection Officer if you receive a request of this nature
- If you have to share highly personal or confidential information, do so in person, over the phone or via a secure file transfer (seek advice from your IT support).
- 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.
- Contact the DPO / Headteacher immediately if you think personal data has been lost, stolen or wrongly disclosed.

STAFF NAME: _____

ROLE: _____

SIGNATURE: _____

DATE: _____