Dallimore Primary & Nursery School

Information Security Protocol – Staff and Pupils

1 Introduction

Information Security is everyone's responsibility. Personal and sensitive data is used, stored, shared, edited and deleted every day. This protocol explains staff responsibilities that are already part of contracts of employment and reflect statutory responsibilities. Details of how personal data is used is contained within the school's Privacy Notices and the Data Protection Policy sets out how our statutory obligations are managed.

This protocol applies to all staff (which includes Governors, agency staff, contractors, work experience students and volunteers) when handling Personal Data. A summary of the guidance is issued to staff and Governors on induction and annually to formally agree to and sign to adhere to.

2 Thinking about privacy on a day-to-day basis

Staff must be aware of data protection and privacy whenever handling Personal and Sensitive Data.

3 Sensitive Personal Data

Data protection is about looking after information about individuals. Even something as simple as a person's name or their attendance record is Personal Data. However, some Personal Data is more sensitive. This is called **Sensitive Personal Data** in this policy and in the data protection policy. Greater care about how that data is used is required.

Sensitive Personal Data is:

- information concerning safeguarding and child protection matters;
- information about serious or confidential medical conditions and information aboutspecial educational needs;
- information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegationhas been proved);
- financial information (for example about parents and staff);
- information about an individual's racial or ethnic origin; and
- political opinions;

- religious beliefs or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- genetic information;
- sexual life or sexual orientation;
- information relating to actual or alleged criminal activity; and
- biometric information (e.g. fingerprints used for controlling access to a building).

Staff need to be extra careful when handling Sensitive Personal Data.

4 Minimising the amount of Personal Data that we hold

Restricting the amount of Personal Data we hold to that which is needed helps keep personal data safe. You should never delete personal data unless you are sure you are allowed to do so.

5 Basic IT expectations

Lock computer screens: Your computer screen should be locked when it is not in use, even if you are only away from the computer for a short period of time.

Be familiar with the tech: You should also make sure that you familiarise yourself with anysoftware or hardware that you use. In particular, please make sure that you understand what the software is supposed to be used for and any risks. For example:

- Electronic registers – make sure that students cannot see personal data of classmates – use the correct view
- if you use a "virtual classroom" which allows you to upload lesson plans and mockexam papers for pupils then you need to be careful that you do not accidently upload anything more confidential;
- be extra careful where you store information containing Sensitive Personal Data.

5.1 **Hardware and software not provided by School:** Staff must not use, download or install anysoftware, app, programme, or service without permission from the Head Teacher. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to the school without using the guest wifi.

5.2 **Private cloud storage:** You must not use private cloud storage or file sharing accounts tostore or share school documents.

5.3 **Portable media devices:** The use of portable media devices (such as USB drives, portable hard drives, DVDs)

5.4 **IT equipment:** If you are loaned IT equipment you must make sure that you sign the loan agreement. School's IT equipment must always be returned to the IT Department in the event of you leaving the School.

6 Passwords

6.1 Passwords should be difficult to guess. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else.

6.2 You should not use a password which other people might guess or know, or be able to find out, such as your address or your birthday.

6.3 You must not use a password which is used for another account. For example, you must notuse your password for your private email address or online services for any school account.

6.4 Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

7 Emails

7.1 When sending emails you must take care to make sure that the recipients are correct.

7.2 **Encryption:** If you cannot transfer data to another recipient via a link to the One Drive remember to encrypt external emails which contain Critical Personal Data.

7.3 **Private email addresses:** You must not use a private email address for school related work. You must only use your school address. Please note that this rule also applies to Governors.

8 Paper files

8.1 **Keep under lock and key:** Staff must ensure that papers which contain Personal Data arekept under lock and key in a secure location and that they are never left unattended on desks (unless the room is secure).

8.2 If the papers contain Critical Personal Data then they must be kept in secure cabinets identified for the specified purpose as set out in the table below.

Information held in paperform must not be stored in any other location, for example, child protection information should only be stored in the cabinet in the Head's (**DSL**) room.

Cabinet	**Access**
Child protection - located in the Head's office	Headteacher and DSLs
Financial information - located in the Head/ SBM's office	Headteacher/ SBM
Health information – info available in pupil file/ locked in classroom cupboard/ staff room/ Middays clipboards	Headteacher/ Office/ Teachers / Tas/ Middays

8.3 **Disposal:** Paper records containing Personal Data should be disposed of securely shredding the material and disposing the paper waste in recycling. Personal Data should never be placed in the general waste.

8.4 **Printing:** When printing documents, use locked printer settings. If you see anything left by the printer which contains Personal Data then you must hand it in to the Head of Regulations and Business Development

8.5 **Put papers away:** You should always keep a tidy desk and put papers away when they are no longer needed.

8.6 **Post:** You also need to be extra careful when sending items in the post. Confidential materials should not be sent using standard post. If you need to send something in the post that is confidential, use signed for and recorded delivery if not suitable to be hand delivered. DCC's 'Orange bag' collection can be classed as secure for DCC maintained schools but not for Safeguarding confidential information.

9 Working off site (e.g. school trips and homeworking)

9.1 Staff might need to take Personal Data off the site for various reasons, (for example because they are working from home or supervising a school trip]. This does not breach data protection law if the appropriate safeguards are in place to protect Personal Data.

9.2 For school trips, the trip organiser should decide what information needs to be taken and who will be responsible for looking after it. You must make sure that Personal Data taken off site is returned to the school.

9.3 **Take the minimum with you:** When working away from your school you must only take the minimum amount of information with you. For example, a teacher organising a field trip might need to take with her information about pupil medical conditions (for example allergies and medication). If only eight out of a class of twenty pupils are attending the trip, then the teacher should only take the information about the eight pupils.

9.4 **Working on the move:** You must not work on documents containing Personal Data whilst travelling if there is a risk of unauthorised disclosure (for example, if there is a risk that someone else will be able to see what you are doing). For example, if working on a laptop on a train, you should ensure that no one else can see the laptop screen and you should notleave any device unattended where there is a risk that it might be taken.

9.5 **Paper records:** If you need to take hard copy (i.e. paper) records with you then you should make sure that they are kept secure. For example:

- Ideally documents should be kept in a locked bag or case. They should not be left in a car overnight;

if travelling by car, you must keep the documents out of plain sight. Please be aware that possessions left on car seats are vulnerable to theft when your car is stopped e.g. at traffic lights;

Public Wi-Fi: You must not use public Wi-Fi to connect to the internet. For example, if you are working in a cafe then you will either need to work offline or if use your personal wifi.

9.6 Critical Personal Data should not be taken off the site in paper format save for specified situations where this is absolutely necessary, for example, where necessary for school trips.

10 Using personal devices for school work

10.1 All staff are expected to access TEAMS via their own personal device for access to TEAM groups and school related messages as part of their employment with School.

10.2 To do this you must install Microsoft Authenticator on your device and agree to adhere to the School's IT acceptable use Protocol.

10.3 **Appropriate security measures** should always be taken. This includes the use of firewalls and anti-virus software. Any software or operating system on the device should be kept upto date.

10.4 **Default passwords**: If you use a personal device for schoolwork which came with a default password then this password should be changed immediately.

10.5 **Sending or saving documents to your personal devices:** Documents containing Personal Data (including photographs and videos) should be deleted after use and not be sent to or saved to personal devices.

10.6 **Friends and family:** You must take steps to ensure that others who use your device (for example, friends and family) cannot access anything school related on your device. For example, you should not share the login details with others and you should log out of your account once you have finished working by restarting your device. You must also make surethat your devices are not configured in a way that would allow someone else access to school related documents.

11 What is an Information Security breach?

Information security breaches can happen in a number of different ways. Examples include:-

- sending a confidential email to the wrong recipient
- letters sent to the wrong address with health and SEN data included
- overheard conversations about a member of staff's health
- an unencrypted laptop stolen after being left in a car
- hacking of school systems
- leaving confidential documents containing Personal Data in a car that was stolen

They are examples of personal data breaches. They need to be reported to the school Data Compliance Officer. This includes anything which you become aware of even if you are not directly involved (for example, if you know that document storage rooms are sometimes left unlocked at weekends). The sooner a breach is notified to the right person, the sooner and more effectively it can be managed. A separate policy and procedure details how the School will process a data breach.

In certain situations, it is necessary breach to the Information Commissioner's Office (the data protection regulator) and let those whose information hasbeen compromised know within strict timescales. This is another reason why it is vital that databreaches are reported immediately.

12 Breach of this policy

12.1 Any breach of this policy will be taken seriously and could ultimately result in disciplinary action for a member of staff.

12.2 This policy does not form part of any employee's contract of employment and can be changed or updated at any time.

Appendix A: Protocols and Guidance for the use of Mobile Phones in School

Personal mobile phones and mobile devices

Responsibility

- Mobile phones and personally-owned mobile devices brought into school are entirely at the staff member, pupil's & parents' or visitors own risk. The School accepts no responsibility forthe loss, theft or damage of any phone or hand held device brought into school
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- The recording, taking and sharing of images, video and audio on any mobile phone is prohibited; except where it has been agreed otherwise by the Headteacher eg) for uploading onto the School Dojo.

Staff

- Staff members may only use their phones for personal use during school break times.
- Mobile phones and personally-owned devices will not be used for personal use during lessons orformal school time.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a schoolmobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Visitors

- All visitors are requested not to use a mobile phone in school and to keep their phones on silent.

Pupils' use of personal devices

- The School strongly advises that pupil mobile phones should not be brought into school.
- The School accepts that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety. In these cases the phone must be passed to class teacher/ TA at the start of the school day for secure storage and will be collected by the child at the end of the school day.
- Pupil's mobile phones are not covered by the School's insurance policy and are brought into school at the parents risk.

- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
  ⍰

Digital images and video in school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school parental consent form when their child joins the school and is reconfirmed annually
- We do not identify pupils in online photographic materials or include full names of pupils in any published school materials;
- Staff sign that they have read and adhere to the school's IT and GDPR Protocols which includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission.We teach them about the risks associated with providing information with images, that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Policy Reviewed – Jan 2023

Next Review – Autumn 2025