



Full Governors
29.01.25

Signed 

Information Security Protocol Staff

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 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.

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

These would all need to be reported to the school Data Compliance Officer (the Office Manager). This also 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.

In certain situations it is necessary report the breach to the Information Commissioner's Office (the data protection regulator) and let those whose information has been compromised know within strict timescales. This is another reason why it is vital that you report breaches immediately.

Privacy on a day-to-day basis

You must be aware of data protection and privacy whenever you are handling Personal and Sensitive Data.

- **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,

- safeguarding and child protection matters;
- serious or confidential physical or mental health conditions

- special educational needs
- serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved)
- financial information (for example about parents and staff);
- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature;
- trade union membership;
- genetic information;
- sexual life or orientation;
- actual or alleged criminal activity
- ⊖ biometric information

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

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.

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. To lock your computer screen, press the "Windows" key followed by the "L" key.
- **Be familiar with the tech:** You should also make sure that you familiarise yourself with any software 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
 - if you use a "virtual classroom" you need to be careful that you do not accidentally upload anything more confidential;
 - shared drives – ensure you know where to store information containing sensitive personal data
 - you need to be extra careful where you store information containing Sensitive Personal Data.

Hardware and software not provided or authorised by Portway Infant School

- Staff must not use, download or install any software, app, programme, or service without permission from the IT engineer. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to Portway Infant School IT systems without permission.
- **Private cloud storage:** You must not use private cloud storage or file sharing accounts to store or share Portway Infant School documents.
- **Portable media devices:** The use of portable media devices (such as USB drives, portable hard drives, DVDs) is not allowed.
- **Portway Infant School IT equipment:** All IT equipment, including supply laptops and class iPads must always be signed out and signed back in again when you have finished using them but absolutely by the end of each day unless it has been agreed that you may have it overnight; the form must be completed correctly to indicate this.

- If you think that an item is broken and will no longer work, this must be reported and the item returned to the office in order that the asset register can be updated accordingly

Passwords

- Passwords should be long and 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.
- 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.
- You must not use a password which is used for another account
- You must not use your password for your private email address or online services for any school account.
- Passwords (and any other security credential you are issued with such as a key fob) must be kept secure and confidential and must not be shared with, or given to, anyone else.

Emails

- When sending emails, you must take care to make sure that the recipients are correct.
- Emails to multiple recipients – ensure you do not automatically use “reply all”, consider appropriate use of “cc” and “bcc”.
- If the email contains sensitive personal data, then you should ask another authorised member of staff to double check that you have entered the email address correctly before sending. Also consider password protecting any documents, sending the password on a separate email or sending the email using a secure email account i.e., Egress
- Private email addresses - You must not use a private email address for Portway Infant School related work. You must only use your school address. Please note that this rule also applies to Governors.

Class Dojo and Teachers 2 Parents (T2P)

- Ensure the appropriate permission for a child is in place before posting any photographs or other information on Class Dojo.
- If you are private messaging (class dojo) or texting/emailing (T2P) a parent, ensure you have selected the correct parent. Also check split parent status and parental responsibilities i.e., make sure you are sharing the correct information with the correct parent.

Paper files

- Staff must ensure that papers which contain personal data are kept under lock and key in a secure location and that they are never left unattended on desks (unless the room is secure). Any keys must be kept safe.
- If the papers contain sensitive 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 paper form must not be stored in any other location, for example, child protection information should only be stored in the cabinet in the Designated Safeguarding Lead's (DSL) room.

The cabinets are located around the site as follows.

Cabinet	Access
Child protection - located in the DSL's office	Headteacher/DSL and DDSL
Financial information - located in the school office	Headteacher, Office Manager and administration staff
Personnel records and Single Central Record – located in the school office	Headteacher, Office Manager and administration staff
Governor records – located in the school office	Clerk to Governors

- **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.
- **Printing** - When printing documents, all connections to the main printer are through the use of a code to minimise the risk of confidential information being read or picked up by someone else. If you see anything left by the printer which contains personal data then you must hand it in to the Office Manager straight away. If you are using a satellite printer then ensure nothing confidential is sent or ensure you are there to collect immediately as it is printing.
- **Put papers away** - You should always keep a tidy desk and put papers away when they are no longer needed. All staff have lockable cupboards or desks in which to store papers.
- **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, it must be sent using Royal Mail Special Delivery (tracked and signed for) or equivalent.

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

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.

- **When a staff member works from home**, they should check with the headteacher whether any additional arrangements need to be put in place to ensure the security of data.
- **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 school.
- **Only 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.

- **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 not leave any device unattended where there is a risk that it might be taken.
- **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:
 - documents should be kept in a locked case. They should also be kept somewhere secure in addition to being kept in a locked case if left unattended (e.g., overnight);
 - if travelling by public transport you must keep the documents with you at all times and they should not be stored in luggage racks;
 - 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;
 - if you have a choice between leaving documents in a vehicle and taking them with you (e.g., to a meeting) then you should take them with you and keep them on your person in a locked case.
 - sensitive 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.
- **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 use a data plan.

Using personal devices for school work

- You may only use your personal device (such as your laptop or smartphone) for school work if you have been given permission by the headteacher.
- Even if you have been given permission to do so, then before using your own device for school work you must speak to our IT engineer so that they can configure your device as required.
- **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 up to date.
- **Default passwords** - If you use a personal device for school work which came with a default password then this password should be changed immediately. Please see above for guidance on choosing a strong password.
- **Sending or saving documents to your personal devices** - Documents containing personal data (including photographs and videos) should not be sent to or saved to personal devices, unless you have been given permission by the headteacher. For example, if you saved a school document to your laptop because you wanted to work on it over the weekend, then the document would still be on your computer hard drive even if you deleted it and emptied the recycle bin.
- **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 sure that your devices are not configured in a way that would allow someone else access to school related documents and information

- **When you stop using your device for school work:** If you stop using your device for schoolwork, for example:
 - if you decide that you do not wish to use your device for school work; or
 - if the school withdraws permission for you to use your device;
 - or if you are about to leave Portway Infant School

then, all school documents (including school emails), and any software applications provided by us for school purposes, will be removed from the device. If this cannot be achieved remotely, you must submit the device to the IT engineer for wiping and software removal. You must provide all necessary co-operation and assistance to the IT engineer in relation to this process.

Breach of this policy

Any breach of this policy will be taken seriously and may result in disciplinary action. A member of staff who deliberately or recklessly obtains or discloses Personal Data held by Portway Infant School without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal. However, this policy does not form part of any employee's contract of employment.

We reserve the right to change this policy at any time. Where appropriate, we will notify staff of those changes by mail or email.

Reviewed spring 2025

To be reviewed spring 2027

Appendix 1 - Protocols for the use of phone in school

Responsibility

Mobile phones brought into school are entirely at the staff member, pupil's, parent's or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any mobile phone.

The school reserves the right to search the content of any mobile phone on the school premises where there is reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles 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 explicitly agreed otherwise by the headteacher. All mobile phone use is to be open to scrutiny and the headteacher is to be able to withdraw or restrict authorisation for use at anytime if it is to be deemed necessary.

Staff

All staff mobile phones must be secured in a locked desk.

Staff members may only use their phones during school break times and when children are not present.

Mobile phones will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.

Staff use of mobile phones

Staff are not permitted to use their own mobile phones for contacting pupils, parents/carers or their families within or outside of the setting in a professional capacity.

Staff will use the school landline phone where contact with pupils, parents or carers is required.

A school mobile will be available whilst on educational off-site visits. Alternatively, staff may have permission from the headteacher or the trip supervisor to bring their own mobile phones on trips to be used strictly for communication with the school or for emergency situations.

Bluetooth communication should be 'hidden' or switched off. They will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

If members of staff have an educational reason to allow pupils to use mobile phones or as part of an educational activity, then it will only take place when approved by the senior leadership team.

Staff must not use their personal mobile phone to take photos or videos of pupils and will only use work-provided equipment for this purpose.

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, then a school mobile 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 their own mobile number for confidentiality purposes.

Visitors

All visitors are requested to keep their phones on silent.

Parents and pupils

Where parents or pupils need to contact each other during the school day, they should do so through the school's telephone.

Pupils' use of personal devices

Pupil mobile phones are not be brought into school.

Digital images and videos

In Portway Infant School,

- consent is sought from parents/carers for use of images and videos involving their child joins the school
- pupils are not identified in online photographic materials or include the full names of the pupil
- any photos used on the school website or prospectus, parents/carers will be asked to provide consent
- pupils are taught about how images can be manipulated in their e-safety education programme