



Elston All Saints Anglican/Methodist Primary School Information Security Policy

Information Security Protocol

Introduction

Information Security is everyone's responsibility. Personal and sensitive data is used, stored, shared, edited and deleted each day.

This policy 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. The Data Protection Policy sets out how the school's statutory obligations are managed.

This policy applies to all staff (which includes Governors, agency staff, contractors, work experience students and volunteers) when handling personal data.

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.

Anything which a staff member becomes aware of even if you are not directly involved needs to be reported. 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 to report a breach to the Information Commissioner's Office (the data protection regulator) and notify those whose information has been compromised within strict timescales. This is another reason why it is vital that you report breaches immediately.

Privacy on a day to day basis

Staff must be aware of data protection and privacy whenever they handle 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 and the data protection policy. Greater care about how that data is used is required.

Sensitive Personal Data includes:

- safeguarding and child protection matters;
- serious or confidential physical or mental health conditions
- special educational needs (SEN) information
- details of 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 about parents/carers 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 sexual orientation;
- actual or alleged criminal activity;
- biometric information (e.g. fingerprints used cashless catering).

Minimising the amount of Personal Data held

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. If you would like guidance on when to delete certain types of information please speak to the Head Teacher or School Business Manager.

Basic IT expectations

Lock computer screens:

A staff member's computer screen should be locked when it is not in use, even if they 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. If you are not sure how to do this then speak to IT.

Be familiar with the tech:

Staff should make sure that they familiarise themselves with any software or hardware that they use. In particular, they need to understand what the software is supposed to be used for and any risks. For example:

- Electronic registers – set to the correct view so students cannot see personal data of classmates
- virtual classroom – be careful that confidential information is not uploaded for students to access.
- Shared drives – ensure you know where to store information containing sensitive personal data.

Hardware and software not provided by Elston All Saints Anglican Methodist Primary School

Staff must not use, download or install any software, 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's IT systems without permission.

Private cloud storage: Staff must not use private cloud storage or file sharing accounts to store or share school documents.

Portable media devices: The use of portable media devices (such as USB drives, portable hard drives, DVDs) is not allowed unless those devices have been given to staff by the school and staff have received training on how to use those devices securely. Education Lincs (IT) will protect any portable media device given to you with encryption.

School IT equipment: If staff are given School IT equipment to use (this includes laptops, printers, phones, and DVDs) you must make sure that this is recorded on the school's IT equipment asset register]. School IT equipment must always be returned to the Head Teacher/School Business Manager even if you think that it is broken and will no longer work and the asset register updated accordingly.

Where to store electronic documents and information: Staff must ensure that they only save or store electronic information and documents in the correct location on the school's systems as follows:

- Google drive and the G drive on the school's internal network.

Passwords

Passwords should be long and difficult to guess, for example, staff could use a song lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Passwords should not be disclosed to anyone else.

- Staff should not use a password which other people might guess or know, or be able to find out, such as their address or birthday.
- Staff must not use a password which is used for another account. For example, they must not use a password for their private email address or online services for any school account.
- Passwords (and any other security credential staff 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.

Emails

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

Emails to multiple recipients, staff must be sure to check that they are using the correct 'To' 'CC' or 'BCC' function. All parent emails are sent through the school office email account office@elstonallsaints.notts.sch.uk to be sent bcc. Email can also be sent via the school office through Arbor. School Business Manager will send all parent emails, staff personal work email accounts should not be used.

If the email contains any personal data then staff should ask themselves is this the best communication method. Sometimes it is unavoidable so staff should ensure the email is sufficiently encrypted and ask an authorised staff member to check the email addresses have been entered accurately. When sending personal data over email, staff should consider inputting the information into an attachable document which is password protected.

Staff must not use a private email address for any school related work. A school email address must only be used. This also applies to governors.

Paper files

Keep under lock and key 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 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 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 Head Teacher's (DSL) office	Head Teacher / DSL

Financial information - located in the School business Manager's office	Head Teacher and School Business Manager
Health information and Single Central Register Information etc – located in Head Teacher and School Business Manager's office	Head Teacher and School Business Manager

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, make sure that you collect everything from the printer straight away, otherwise there is a risk that confidential information might be 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 School Business Manager or Head Teacher.

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

Our SENCO is provided with their own personal secure cabinet(s) in which to store papers. However, these personal cabinets should not be used to store documents containing critical personal data. Please see above for details of where Critical Personal Data should be kept.

Post: Staff also need to be extra careful when sending items in the post. Confidential materials should not be sent using standard post. If staff need to send something in the post that is confidential, consider arranging for it to be sent by courier.

Working off site: Staff might need to take personal data off site for various reasons, such as remote working or supervising a school trip. This does not breach data protection law if the appropriate safeguards are in place to protect personal data.

For school trips, the trip supervisor should decide what information needs to be taken and who will be responsible for looking after it. Any personal data taken off site is returned back to school.

When a staff member works from home they should check with the Head Teacher what additional arrangements are in place to protect personal data.

Take the minimum with you: When working away from school staff must only take the minimum amount of information with them. For example, if 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: Staff must not work on documents containing personal data whilst travelling if there is a risk of unauthorised disclosure. For example, if working on a laptop on a train, the individual should not leave any device unattended where there is a risk of theft.

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

- documents should be kept in a locked case.
- Information should be kept with them at all times
- The individual must keep documents out of plain sight
- If the individual has a choice between leaving documents in a vehicle and taking them with them (e.g. to a meeting) then they should be taken with them.

Public Wi-Fi: Staff must not use public Wi-Fi to connect to the internet. For example, if you are working in a public café, staff will either need to work offline or use 4G / 5G.

Using school laptops, phones, cameras and other devices: If you need to book out an additional school device please complete a proforma and ensure it is signed by the Head Teacher.

Using personal devices to access school work

Staff may only use their personal device (such as laptop or smartphone) for school work if they have been given permission by the Head Teacher.

Even if they have been given permission to do so, then before using their own device they must speak with Education Lincs so that they can configure the device.

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 a personal device for school work came with a default password then this password should be changed immediately.

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. This is because anything saved to a computer, tablet or mobile phone will not be protected by the school's security systems. Furthermore, it is often very difficult to delete something which has been saved to a computer. For example, if staff saved a school document to their laptop because they wanted to work on it over the weekend, then the document would still be on their computer hard drive even if they deleted it and emptied the recycle bin.

Friends and family: Staff must take steps to ensure that others who use their device (for example, friends and family) cannot access any school related information. Staff must ensure that the device is not configured in a way that would allow someone else access to school related documents and information – if they are unsure about this then they need to contact Education Lincs who can assist with this.

When staff stop using their device for school work: If staff stop using their device for school work, all documents including emails and software applications provided by the school must be removed from the device.

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 the school without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

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.

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 for the 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 explicitly agreed otherwise by the Head Teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head Teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

Mobile phones and personally-owned devices approved for use by the Head Teacher in exceptional circumstances are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.

Staff

All staff mobile phones must be secured in the staffroom or their personal bag.

Staff members may use their phones during school break times in certain areas.

Mobile phones and personally-owned devices 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 personal devices

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

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

Staff may have permission from the Head Teacher to bring their own mobile phone on trips to be used strictly for communication with the school or for emergency situations.

Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices 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 children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.

Staff should not use personally-owned devices, such as mobile phones or cameras, 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, or for contacting pupils or parents, they should use their own device and hide (by inputting 141) 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 only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school business manager to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

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 particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.

If a pupil breaches the school policy then the phone or device will be removed and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

No pupils should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be held in the school office until the end of the school day.

Digital Images and Videos

- consent is sought from parents/carers for use of images and videos involving their child as part of the admission process when their child joins the school
- pupils are not identified in online photographic materials or include the full names of the pupil
- staff confirm that they have read and understood this policy
- any photos used on the school website, parents/carers will be asked to provide consent
- pupils are taught about how images can be manipulated in their e-safety education programme
- pupils are advised to be very careful about placing any personal photos on any 'social' online network space.
- Pupils are taught that they should not post images or videos of others without their permission.

Reviewed January 2026

Next Review September 2026

Information Security Policy

I confirm that I have read and understood the contents of this policy.

Name	Signature	Date