Information Security Policy



Reviewed: November 2026

Next review: November 2027

About this policy

This policy explains how Kingsley Primary School keeps information safe – on paper, on computers and online. It applies to everyone who works or volunteers at the school. It also explains how anyone can ask to see information we hold.

In short

- Only people who need information for their job can see it.
- Everyone has their own account and a strong password and, where needed, a second check such as a code on their phone.
- School information stays on school systems – not on personal phones, personal email or personal cloud storage.
- If something goes wrong, such as a lost laptop, a suspicious email or information sent to the wrong person, tell the headteacher or leadership straight away.
- Anyone can ask to see the information we hold about them, or ask for information about how the school is run.

For staff and governors: you must follow this policy. If you are unsure about anything, ask the headteacher or leadership or our Data Protection Officer (DPO).

Kingsley Primary School must follow data protection law. This protects people's personal information and limits who we can share it with. Personal information is anything that can identify a living person, such as a name, address, date of birth, pupil number or photograph.

Pupils, parents, staff and others trust us with their information. Everyone who works for the school must treat that information with respect, keep it confidential, and only use it in fair and open ways that the law allows.

Keeping information secure means three things:

Confidentiality –only the people who are allowed to see information can see it.

Integrity –information is accurate and complete, and is not changed or lost by mistake.

Availability – information and systems are available to the people who need them, when they need them.

Who and what does this policy cover?

This policy applies to all staff (including temporary, supply and agency staff), governors, volunteers, contractors and anyone else who uses the school's information or IT systems.

It covers information in every form, including:

- Paper documents and printouts
- Information stored on computers, including scanned documents
- Post, email and files sent electronically
- USB sticks, memory cards, CDs and other removable storage
- Laptops, tablets, mobile phones and cameras
- Conversations, phone calls, voicemails and recordings

- Our website and other information we publish online
- Photographs and videos
- Cloud services and online systems the school uses, such as our school management system and learning platforms
- Personal devices used for school work, where this is allowed

This policy also covers:

- Keeping our systems and devices secure, including passwords, backups and protection against cyber attacks
- People's rights to see the information we hold about them
- Requests for information about how the school is run (freedom of information)
- Keeping a record of the information we hold

Other policies give more detail on related topics, including our Data Protection Policy and Acceptable Use Policy

Why do we have this policy?

This policy helps us to:

- Take a clear, consistent approach to keeping information safe
- Prevent problems such as misuse of information or attacks on our computers, spot them quickly if they happen, and deal with them properly
- Protect the school's reputation and meet our legal and ethical responsibilities
- Respect the rights of pupils, parents, staff and others, and deal properly with any complaints or questions about how we handle information
- Meet the legal requirement to keep personal information secure, and the Department for Education's (DfE) cyber security standards for schools

Who looks after data protection?

We handle personal information in line with data protection law. Our Data Protection Policy explains this in full.

The school is responsible for the personal information it holds (in law, this makes us the "data controller"). We pay the data protection fee to the Information Commissioner's Office (ICO), the UK's data protection regulator. Our registration number is Z6036245. We also have a Data Protection Officer (DPO), whose contact details are:

Data Protection Officer
ADNS Group
5 Eggleston Court,
Riverside Park, Middlesbrough
TS21RU
Compliance@adnsgroup.com

03003033793

***Please ensure you include the name of the school in all correspondence with the DPO**

The law requires us to have a DPO. The DPO gives advice and reports to the governing board and the headteacher. The DPO:

- Is the main contact for the ICO and for anyone with a question about their information
- the school review its record of the information it holds, and its information policies
- Helps report and investigate security incidents and data breaches
- Gives advice on data protection, including requests for information, sharing information, and checking the risks of new systems
- Reports to governors on these matters

Who is responsible for what?

Everyone who uses school information must help keep it safe. In particular:

- The governing board is responsible overall and approves this policy.
- The headteacher makes sure this policy is followed, and that security incidents and data breaches are reported.
- The DPO gives advice and checks we are following the law.
- Our IT support provider, ADNS looks after the technical security of our systems.
- All staff, governors and volunteers must follow this policy, complete their training and report any concerns straight away.

Who can see information?

People can only see the information they genuinely need for their job. Access to protected systems must be approved by the Headteacher or leadership. An email from them approving access counts as approval.

What this means for staff:

- Everyone has their own account. Never share your account or password.
- You will only be given access to what you need, and this is checked at least once a year.
- Your access changes when your role changes, and is removed on your last day if you leave.
- Use a strong password. For email, cloud systems, working from home and administrator accounts, you will also need a second check, such as a code on your phone (multi-factor authentication).
- Lock your screen whenever you leave your computer.

How sensitive is the information?

We sort information into three groups, so everyone knows how carefully to handle it:

High risk – information about people, especially sensitive information such as health, SEND and safeguarding records, plus finance, payroll and staff records.

Confidential – information that is not about people but still should not be shared, such as contracts, security details and governing board papers that have not been published.

Public – information anyone can see, such as what we publish on our website.

High risk information must only be kept on school systems. It must be encrypted (protected so it cannot be read without a password or key) if it is sent outside the school or taken off site. It must never be kept on personal devices or in personal email or cloud accounts.

How do we keep our systems secure?

Our computers and systems are protected in line with the DfE's cyber security standards for schools and good practice. They must have:

- Up-to-date antivirus protection
- A firewall, which blocks unwanted access from the internet
- Encryption on all laptops and USB sticks
- The latest security updates, and no out-of-date software that no longer receives updates
- Multi-factor authentication, as explained above
- Regular backups, including at least one copy kept separate from the school network, which are tested

Each year we also check our cyber security risks and update our plan for what to do if our systems are attacked or stop working. We are registered with Police CyberAlarm, a free police service that helps spot attacks. These are also conditions of the DfE's Risk Protection Arrangement (RPA) cyber cover.

What training do staff get?

All staff and governors complete data protection and cyber security training when they join and at least once a year. This includes the National Cyber Security Centre's (NCSC) training for school staff. We regularly remind staff how to spot scam (phishing) emails.

Can staff work from home or use their own devices?

If you work away from school, use school devices or the school's approved secure remote access. Do not save school information on personal devices, in personal email or in personal cloud storage. Keep devices secure and out of sight when travelling, and do not let family members use them.

Can staff use AI tools?

Do not put personal information or confidential school information into AI tools, such as chatbots, unless the school has approved the tool and, where needed, checked the risks first. You are responsible for checking anything an AI tool produces.

How do we keep track of the information we hold?

With advice from the DPO, we keep a list of the main sets of information we hold, called an information asset register. This is also the record of our use of personal information that the law requires. For each set of information, it records:

- A reference number
- Who is responsible for it
- What it is and why we have it
- Whether we have told people how we use it (a privacy notice)
- What form it is in and where it is kept
- Which staff (by job title or team) normally use it
- Any agreements for sharing it with other organisations
- Our legal reason for using it
- Any outside companies that handle it for us
- How long we keep it

The register is reviewed every year. The headteacher will tell the DPO as soon as possible about any big changes, such as a new system or supplier. Before we bring in a new system or way of working that could put people's information at high risk, we check the risks first (a data protection impact assessment).

Who is responsible for each set of information?

Each main set of information has an owner. This is a senior member of staff who understands why the information matters and what the risks are.

Owners make sure their information is kept secure and that other staff use it safely. They also make sure it is kept for the right length of time under our Records Management and Retention Policy, and destroyed securely when it is no longer needed.

How can people see the information we hold about them?

Anyone can ask to see the personal information we hold about them. This is called a subject access request. It can be made in person, by phone or in writing, and does not need a special form. It is free, unless someone asks for extra copies or makes requests that are clearly unreasonable or excessive.

If someone else, such as a solicitor, asks on a person's behalf, we need written proof of who they are and that the person agrees. We only ask for proof of identity if we are unsure who is asking.

We will reply within one month. For complicated requests, this can be extended by up to two more months, and the time limit is paused while we wait for any details we need. Our reply will:

- Tell the person whether we hold information about them
- Give them a copy of it
- Explain why we use it, who we share it with, how long we keep it, where it came from, and their rights

Parents also have a separate right to see their child's school record within 15 school days. Our Data Protection Policy explains how we handle requests in full.

When might we share confidential information?

We may share confidential information without permission when:

- The person who gave us the information, and the person it is about, have agreed
- The information is already publicly available
- The information does not identify anyone, such as statistics
- There is a serious risk of harm to the person, for example if they are at risk of suicide
- There is a risk of harm to others. For example, any concern that a child may be at risk of abuse must be passed to the Designated Safeguarding Lead (DSL), who will decide whether to contact children's social care or the police. Our Child Protection and Safeguarding Policy explains this in more detail.
- It will help prevent a serious crime, especially where people could be put in danger
- The law or a court requires us to share it

Data protection law never stops staff sharing information that is needed to keep a child safe. Any decision to share information, and the reason for it, must be written down.

How can people ask for information about the school?

Anyone can ask for information about how the school is run, under the Freedom of Information Act 2000 (FOI). Requests for environmental information are made under the Environmental Information Regulations 2004 (EIR).

Send your request to the school office at admin@kingsleyschool.org.uk or by post. If you need help making a request, call the school office on 01429 273102.

What does the headteacher do?

The headteacher is responsible for:

- Checking whether we hold the information
- Finding and gathering it
- Deciding whether the law allows any of it to be withheld, including whether releasing it is in the public interest
- Preparing the information and the reply
- Getting the reply approved
- Sending the reply

How do I make a request?

- Freedom of information requests must be in writing, which includes email. Please give your real name and an address for our reply (an email address is fine). For security reasons, we will not open links or attachments in requests.
- Requests for environmental information can also be made in person or by phone. We will confirm the details with you in writing.

We will acknowledge your request within 5 school days. If we are thinking of withholding information, or are unsure whether the law allows us to, the Chair of Governors and the headteacher will decide together. They will:

- Write down the reasons for and against releasing the information
- Look at how similar cases have been decided, if needed
- Ask the DPO for advice

The reasons for these decisions will be reported to the next governing board meeting.

What do we publish, and is there a charge?

We follow the ICO's model publication scheme for schools, and publish as much information as we can on our website.

Most requests are free. We may charge for things like photocopying and postage. If so, we will tell you in writing first, and you will need to pay before we send the information. If finding and preparing the information would cost more than £450 (about 18 hours of work), we may refuse the request, but we will help you narrow it down. Charges for environmental information must be reasonable. We follow the local authority's approach to charging for these requests.

How long will it take?

We will reply to freedom of information requests within 20 school days, or 60 working days if that is sooner. We will reply to environmental information requests within 20 working days, or 40 working days if the request is complex or large.
If you are unhappy with our reply, you can ask for it to be reviewed by the Chair of Governors. If you are still unhappy, you can complain to the ICO.

How should staff look after paper records and devices?

Keep notes, records and other sensitive information secure, and lock them away after use. Make sure you know any extra rules for recording and storing information that apply to your role.

In particular:

- Keep your desk clear of personal information, and lock your screen, when you are away from it.
- Only take paper records off site when you need to. Carry them securely, keep them out of sight, and never leave them unattended or in a car overnight.
- Print securely and collect printouts straight away.
- Shred paper containing personal information, or put it in the confidential waste. Old IT equipment must be disposed of by an approved company, and the certificate of destruction kept.

What should I do if something goes wrong?

If you think there has been a data breach, cyber attack or other security problem – for example a lost device, a suspicious email, or information sent to the wrong person – tell the headteacher or leadership immediately. Do not wait until you are sure. The school will contact the DPO straight away.

If a breach could put people at risk, the school must report it to the ICO within 72 hours. Cyber attacks are also reported to Report Fraud (formerly Action Fraud) and, if the school is an RPA member, to the RPA emergency helpline. Our Data Protection Policy explains this in full.

When is this policy reviewed?

This policy is reviewed every year by the headteacher and the DPO and approved by the governing body.

The legal detail

This section lists the formal legal references behind this policy.

Data protection

- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018), as amended by the Data (Use and Access) Act 2025
- Security of personal data: UK GDPR Article 5(1)(f) and Article 32
- Record of processing activities: UK GDPR Article 30, met by the information asset register
- Data protection impact assessments: UK GDPR Article 35
- Subject access requests: UK GDPR Articles 12 and 15. One month to respond, extendable by up to two months for complex requests. A fee may only be charged for further copies, or for manifestly unfounded or excessive requests
- Personal data breaches: reported to the ICO within 72 hours where there is a risk to individuals (UK GDPR Article 33)
- Educational records: Education (Pupil Information) (England) Regulations 2005

Freedom of information

- Freedom of Information Act 2000 and Environmental Information Regulations 2004
- Freedom of Information (Time for Compliance with Request) Regulations 2010: 20 school days or 60 working days, whichever is sooner
- Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004: appropriate limit of £450, at £25 an hour
- ICO model publication scheme for schools

Cyber security and safeguarding

- DfE: Meeting digital and technology standards in schools and colleges (cyber security standards)
- DfE Risk Protection Arrangement (RPA) cyber cover conditions
- Keeping Children Safe in Education (statutory guidance)