

Information Security Policy



Table of Contents

Policy Statement	3
Scope.....	3
Purpose	4
Data Protection	4
User Access Controls & Authorisation	5
Data Classification	5
Basic Data Protection Requirement.....	5
Information Asset register	5
Information asset owners	5
Requests by data Subjects for Access to Data Held.....	6
Breaking Confidentiality.....	6
Access to Information	6
Responsibilities of the Headteacher:	7
How to Submit a Request:	7
Publication Scheme and Charges:.....	7
Response Times:	7
Confidentiality and the keeping and transport of sensitive information	7

Policy Statement

Kingsley Primary School is bound by the UK's Data Protection Act which implements the EU Data Protection Directive. This protects personal data and places restrictions on Tennants ability to disclose personal data within the UK and overseas. Personal Data is information relating to an individual from which they can be identified, e.g. name, address, tax details or national insurance number.

The school's staff will often be entrusted with personal information given to them in confidence by individuals using our services. Anyone working for the school has a duty to treat that information with respect. They also have a duty under the Data Protection Act 1998 to protect the confidentiality of personal information and to process that information fairly and transparently.

Information security is deemed to safeguard three main objectives:

Confidentiality – Data and information assets must be confined to people authorized to access and not be disclosed to others;

Integrity – Keeping the data intact, complete and accurate, and IT systems operational;

Availability – An objective indicating that information or system is at disposal of authorized users when needed.

Scope

The information policy applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper.
- Information or data stored electronically, including scanned images.
- Communications sent by post/ courier or using electronic means such as email fax, or electronic file transfer.
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card.
- Information stored on portable computing devices including mobile phones, tablets, cameras, and laptops.
- Speech, voice recordings and verbal communications including voicemail.
- Published web content, for example intranet and internet.
- Photographs and other digital images.

This policy is the schools main information governance policy and addresses:

- Data protection (including rights and complaints)
- Freedom of information
- Information Asset register

Information security, acceptable use of systems, records management and security incident reporting will be addressed in separate policies.

Purpose

- To establish a general approach to information security
- To detect and forestall the compromise of information security such as misuse of data, networks, computer systems, and applications.
- To protect the reputation of the company with respect to its ethical and legal responsibilities.
- To observe rights of the customers; providing effective mechanisms for responding to complaints and queries concerning real or perceived non-compliances with the policy is one way to achieve this objective.

Data Protection

Personal data will be processed in accordance with the requirements of the GDPR in compliance with the data protection principles specified in legislation.

Kingsley Primary School has notified the information Commissioners office that is a data controller and has appointed a Data Protection Officer (DPO). Details of the DPO can be found here.

Data Protection Officer
Scott Thornhill
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 DPO is a statutory position and will operate in an advisory capacity. Duties will include:

- Acting as the point of contact for the information Commissioner's Office (ICO) and data subjects
- Facilitating a periodic review of the corporate information asset register and information governance policies
- assisting with the reporting and investigation of information security breaches
- providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and
- reporting to governors on the above matters.

User Access Controls & Authorisation

Access to information shall be restricted to authorised users who have a Bonafede need to access information. Authorisation for access to restricted applications and databases must be granted by the designated person. An electronic mail message from the designated persons mail account granting authorisation for appropriate access shall constitute such authorisation.

Data Classification

High risk class- data protected by state and federal legislation(the Data Protection Act) as well as financial, payroll and personnel (privacy requirements) are included here.

Confidential class- the data in this class does not enjoy the privilege of being under the wing of law, but the data owner judges that it should be protected against unauthorised disclosure.

Class public- this information can be freely distributed.

Basic Data Protection Requirement

Systems hosting personal information must be protected in alignment with the schools' standards and industry best practise. Specifically, the systems must operate:

- Up to date anti-malware protection
- A firewall
- Encryption
- Be appropriately patched

Information Asset register

The DPO will advise the school in developing and maintaining an information asset register (IAR). The register will include the following information for each asset:

- An individual information asset identification number
- The owner of that asset
- Description and purpose of the asset
- Whether there is a privacy notice published for that asset
- Format and location of the asset
- Which officers (job titles/ teams) have routine access to the information
- Whether there are any data sharing agreements relating to the information and the name of that agreement.
- Conditions of data processing
- Details of any third parties contracted to process the information.
- Retention period for the asset.

The IAR will be reviewed annually and the headteacher will inform the DPO of any significant changes to their information assets as soon as possible.

Information asset owners

An information asset owner (IAO) is the individual responsible for an information asset, understands the value of that information asset, understands the value of that information and the potential risks

associate with it. The school will ensure that the IAO's are appointed based on sufficient seniority and level of responsibility.

IAO's are responsible for the security and the maintenance of their information assets. This includes ensuring that other members of staff are using the information safely and responsibly. The role also includes determining the retention period for the asset, and when destroyed, ensuring this is done so securely.

Requests by data Subjects for Access to Data Held

If an individual wish to see any personal information about them held by the school , this can be shown to him or her and a copy made if one is requested. If a third party (such as a solicitor) is acting on behalf of an individual, proof of the third party's identity and the individuals authority to disclose their information to their representative, must be obtained in writing. There may be an administrative charge made for this service. All requests must be responded to within 20 working days and the following must be adhered to:

- To tell the applicant whether you hold any information falling within the scope of their request; and
- To provide that information

Breaking Confidentiality

Confidentiality may be broken by the following circumstances.

- Threat to Self.
- Threat to Others.
- Suspicion of Abuse.
- Where consent is given by the person from whom the information was obtained, and (if different) the person to whom it relates
- Where the information is already available to the public from other sources
- Where the information is in the form of a report or collection of information where it is not possible to ascertain from it information relating to any particular person (eg in a service report providing statistical information)
- When there is a serious risk of harm to the individual, as in a threatened suicide
- To protect others, for example, information about possible child abuse should be disclosed to the appropriate agency. The *Alliance Safeguarding Children Policy* gives further information about this specific issue
- To prevent a serious criminal act, especially where others may be endangered, for example an act of terrorism.

Access to Information

Requests for Information under the Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations 2004 (EIR)

Requests for information under these legislations should be directed to the school office by calling 01429 273102

Responsibilities of the Headteacher:

The Headteacher is responsible for:

- Determining whether the requested information is held.
- Locating, retrieving, or extracting the requested information.
- Assessing whether any exemptions apply and weighing the public interest test.
- Preparing the materials for disclosure and drafting the response.
- Obtaining necessary approvals for the response.
- Sending the response to the requester.

How to Submit a Request:

- FOIA requests must be made in writing. Requests must include a valid name and address; we will not process requests that require clicking on electronic links.
- EIR requests may be made verbally, but we will follow up in writing with the requester to confirm the details and ensure accuracy.

Each request will be acknowledged within 5 school days. The Chair of Governors and Headteacher will jointly consider cases requiring a public interest test or where there is uncertainty about applying an exemption. When applying the public interest test, they will:

- Clearly document the benefits of both disclosing and withholding the information.
- Refer to relevant case law to determine where the balance lies, if necessary.
- Consult the Data Protection Officer (DPO).

Reasons for decisions to disclose or withhold information will be reported at the next governing body meeting.

Publication Scheme and Charges:

We follow the Information Commissioner's model publication scheme for schools and aim to publish as much information as possible on our website to promote transparency and accountability.

Charges for providing information may be applied in line with current regulations. Applicants will be notified in writing if a fee applies, and payment must be received before the information is provided. Kingsley Primary School adheres to the Local Authority's charging regime for FOI/EIR requests.

Response Times:

We comply with FOI/EIR timescales and aim to respond to requests within 20 school days.

Confidentiality and the keeping and transport of sensitive information

All notes, records and other sensitive information must be kept securely and locked away after use. Workers should make sure they are aware of any specific service requirements regarding recording and storing information relevant to their specific role.