Thurlstone Primary School
Information & Data Security Policy

Data Security is a key element of ensuring that data collected by the school and processed on electronic systems is done in line with the Data Protection Act (2018) and the 'UK-GDPR'. It ensures that appropriate measures are taken by the school so that data processed on internal and external systems are in line with key data security principles to minimise any data breach.

The school is dedicated to ensure the security of all information that it holds and implements the following measures to achieve this:

- Protect against potential breaches of confidentiality
- Ensure that all information assets and IT equipment/infrastructure are protected against damage, loss or misuse
- Support our Data Protection Policy in ensuring all staff are aware of and comply with UK GDPR and our own procedures applying to the processing of data
- Increase awareness and understanding at Thurlstone Primary School of the requirements of information security and the responsibility to staff to protect the confidentiality and integrity of the information that they handle. All staff are responsible for keeping information secure in accordance with the legislation and must follow the school's acceptable usage policy.

Introduction

Information security can be defined as *the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction*. Staff are referred to the Data Protection Policy, Data Breach Policy, Data Retention Policy and e-Safety Policy for further information.

For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, laptops, iPads, tables, digital cameras, memory sticks, smartwatches and smartphones.

Scope

The information covered by this policy includes all written, spoken and electronic information that is held, used or transmitted by or on behalf of the school in whatever media. This includes information held on computer systems, cloud based systems, paper records, hand held devices and information transmitted orally.

This policy applies to all members of staff, including temporary staff, other contractors, volunteers, governors and any other third party authorised to us the IT systems of the school. All staff are required to familiarise themselves with its content and comply with the provisions contained in it.
Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the school's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

Staff are also protected via the school's Whistleblowing Policy, if they see a member of staff not adhering to the IT security procedures and acting in a way that could compromise data protection.

Principles
Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

- **Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.
- **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users can access the personal data when they need it for authorised purposes.
- Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with the UK -GDPR.

All IT systems are to be installed, maintained, repaired and upgraded by the school's IT consultants.

All Data stored on our IT systems and paper records shall be available only to members of staff with a legitimate need for access.

All staff have an obligation to report actual or potential data protection compliance failures to the School Business Manager or headteacher, who will investigate the breach. This must be done within 72 hours of a compliance failure. Any breach which is either known or suspected to involve personal or sensitive data shall be reported to the DPO.

Data Privacy Impact Assessments
In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:
https://icosearch.ico.org.uk/s/search.html?query=privacy+impact+assessments&collection=ico-meta&profile=_default
https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/consultation-on-the-conducting-privacy-impact-assessments-code-of-practice/

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

If a member of staff is conducting any high risk data action that could lead to a data breach, then they must discuss this matter with the business manager. This could include taking data offsite or sharing data with a third party organisation. The external company may be asked to complete a DPIA or the school will speak to the DPO regarding the completion of the risk assessment.

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

In line with UK-GDPR, the school will need to ascertain whether a Standard Contractual Clause (SCC) is needed for the sharing of data with a 'third country'.

The security arrangements of any organisation with which data is shared shall also be considered and these organisations shall provide evidence of the competence in the security of shared data.

Physical Security and Procedures

Paper records and documents containing personal information, sensitive personal information and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible. At the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available locked filing cabinets and locked cupboards shall be used to store paper records when not in use. Paper documents containing confidential information should not be left on office or classroom desks, on staffroom tables, or pinned to notice boards where there is general access unless there is a legal reason to do so and or when relevant consent has been provided. You should take particular care if documents have to be taken out of school.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find security to be insufficient, you must inform the headteacher as soon as possible. The school has access control installed all access doors into the building. Only authorised staff and contractors are provided with a fob to access these doors.

The school has an intruder alarm system installed which is set nightly, over the weekends and during school holiday periods. CCTV cameras are installed in various locations around the school premises and is monitored by the school office.

All visitors are required to sign in the electronic visitor management system. [explain here where visitors data is kept and for how long] and are accompanied by a member of staff and not left alone in areas where they could have access to confidential information.

Electronic Storage of Data

All portable data, and in particular personal data, should be stored on encrypted drives. All teacher laptops and desktops are bitlocker encrypted. Data should only be stored on the school network and not on any local drives to allow the data to be backed up.

Home working

You should not take confidential or other information home without prior permission from the Headteacher and only do so where satisfied appropriate technical measures are in place to maintain continued security and confidentiality of that information. A Privacy Impact Assessment must be completed and signed by the Headteacher prior to the information being taken home.
When you have been given permission to take confidential or other information home, you must ensure that:

- The information is kept in a secure and locked environment where it cannot be accessed by family members or visitors
- All confidential material that requires disposal is shredded or in the case of electronic material, security destroyed as soon as any need for its retention has passed. Please refer to the school's Retention Policy for further details.
- The information is not transported in see-through or other un-secured bags or cases
- The information is not read in public places (e.g. waiting rooms, cafes, public transport etc.
- Where possible, staff to access the information via Forticlient using their secure login

Computers and IT

All members of staff are responsible for:

- complying with all relevant parts of this policy at all times when using IT systems and equipment
- Adhere to and sign the IT Acceptable Usage Policy found in the e-Safety Policy. If staff or pupils discover unsuitable sites or any material which would be unsuitable, this must be reported immediately to a member of SLT.
- All Computers and laptops must be locked using the Ctrl/Alt/Delete command or Windows L when not in use to minimise the accidental loss or disclosure of information. Staff should be aware if they fail to log off and leave their computers/laptops unattended they may be held responsible for another user's activities on their terminal and be in breach of this policy, the Data Protection policy and or the requirement for confidentiality in respect of certain information.
- All staff must provide accurate and up to date information regarding their employment and keep the school informed of any changes to information that they have provided e.g. change of address, contact telephone number etc. The school cannot be held responsible for any such errors unless the staff member has informed the school of such changes.
- Any personal data that is held is kept securely either in a locked cabinet/drawer and if electronic, be password protected and backed up regularly. No personal data is allowed to be stored on a pen drive or on the local hard drive of teacher laptops. Personal data can only be stored on the school network and the Data Protection Officer provided with an Evidence Sheet to monitor where data is stored. All Teacher laptops are encrypted and Bitlocker security protected.
- Personal information must not be disclosed either orally or in writing or via web pages or by any other means, accidentally or otherwise to any unauthorised third party. Sensitive and personal printed documents should not be left at printers or in public areas.
- Personal information sent to authorised third parties must be sent using Cryptshare or Office 365 Encrypt tool. This is done by typing the word 'Encrypt' into the subject field or body of the message being sent.
- Pupil information sent to other schools must be sent via the school management system by generating a ctf file. This file type can only be opened using the transferring school's management information system which requires a secure login to access.
- Staff should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- Staff are required to use a secure login to access the network and school data and are not permitted to install any software on computers/laptops. This can only be done by the school's IT service provider who ensure the software does not pose any risk to the security and integrity of the network.
- Staff should follow the school policy in ensuring that passwords [enter school password procedures]

The IT consultant shall also be responsible for:

- ensuring that all IT systems are assessed and deemed suitable for compliance with the school's security requirements and that IT security standards are effectively implemented and regularly reviewed, working in consultation with the schools management and reporting any concerns to them.
- Ensuring that all members of staff are granted levels of access to IT systems that are appropriate for each member, taking into account their job role, responsibilities and any special security requirements
- Receiving and handling all reports relating to IT security matters taking appropriate action in response
- Monitoring all IT security within school and taking all necessary action to implement this policy

- The School has implemented an internet filtering system which is managed by our IT consultants who are responsible for performing regular checks to ensure that filtering is appropriate.
- Ensuring that regular backups are taken of all data stored within IT systems and that the backups are stored appropriately offsite.
- Following data security procedures and regularly patching software to minimise any security breach.
- To inform the school immediately about any potential data breach from a cyber-attack or ransomware.

The school management are responsible for:

- ensuring that access to the school information management system will be on a need-to-know basis
- all information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know basis.
- ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations including but not limited to UK GDPR.

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

Bring Your Own Device (BYOD)

Staff are only authorised to use their own device if they complete and sign the BYOD agreement. (Please see BYOD Agreement Document)

Reporting security breaches

All concerns, questions, suspected or known breaches shall be referred immediately to the Headteacher/SBM who will report to the DPO. All members of staff have an obligation to report actual or potential data protection compliance failures.
Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information must be reported immediately to the Headteacher or SBM.

Please refer to the school's Data Breach Policy for further information.

Business Continuity

In the event of a cyberattack or ransomware, the school will work with its IT technical support to ensure that no data is compromised or breached.

Data Access Requests (Subject Access Requests)

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within 1 month and they should be made in writing to: Headteacher [name of school]

The school will ask to see evidence of your identity, such as your passport or driving licence before disclosure of information.

https://ico.org.uk/media/for-organisations/documents/1586/personal_information_online_small_business_checklist.pdf

https://ico.org.uk/media/for-organisations/documents/1235/definition-document-schools-in-england.pdf

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some information about pupils to the Local Authority and the Department for Education (DfE). If you want to see a copy of the information about you that we hold and/or share, please contact **the School Office**

Related Policies to be read in conjunction with this policy:

- Acceptable Usage Policy
- e-Safety Policy
- UK GDPR & Data Protection Policy
- Data Breach Policy
- Data Retention Policy
- Safeguarding Policy
- Freedom of Information Act Policy