PINNER PARK INFANT & NURSERY SCHOOL

Data Protection and Security Policy

Pinner Park Infant and Nursery School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with the statutory obligations of Local Authorities (LAs), government agencies and other bodies.

The Data Protection Act (DPA) 1998 is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities under the Data Protection Act and will comply fully with it.

The policy will be communicated to all staff and they will be expected to understand and abide by it.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and, where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose;
6. Personal data shall be processed in accordance with the rights of data subjects under the act;
7. An appropriate degree of security shall be used to ensure the protection of personal data through the use of appropriate technical and organisational measures against unauthorised or unlawful processing of the personal data and against accidental loss or destruction of, or damage to, the data;

8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected;
- Inform individuals when their information is shared, and why and with whom it was shared;
- Check the quality and the accuracy of the information it holds;
- Ensure that information is not retained for longer than is necessary;
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely;
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- Share information with others only when it is legally appropriate to do so;
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests;
- Ensure all staff are aware of, and understand, our policies and procedures.

Summary

This policy is complimentary to the school's **Appropriate Use of Computing Systems Policy** and is intended for all who use, or support, the school's IT systems or data, to ensure:

- the protection, confidentiality, integrity and availability of school information and assets;
- all users are aware of, and fully comply with, all relevant legislation;
- all staff understand the need for information and IT security and understand their responsibilities in respect to this.

Definitions

• ***Information*** – covers any information, including electronic capture and storage, manual paper records, video and audio recordings, and any images, however it is created.

• ***Personal Data*** – data that can be used to identify a living person; this includes names, birthday and anniversary dates, addresses, telephone numbers, fax numbers, email addresses and so on; it applies only to data that is held, or intended to be held, on computers (equipment operating automatically in response to instructions given for that purpose), or held in a 'relevant filing system', this includes paper filing systems.

• ***Strong Password*** – a password that is at least eight characters in length, contains upper and lower case alphabetical characters and numbers or punctuation characters.

• ***Encryption*** – the process of transforming information (plaintext) using an algorithm (a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

- ***USO Nominated Contact*** – a member of staff nominated by the school to work with Atomwide / LGfL and the school's MIS to maintain the school's Unified Sign On (USO) accounts.

Responsibilities:

- The School shall be registered with the Information Commissioner's Office (ICO–see http://www.ico.gov.uk/)under the 1998 Data Protection Act.
- Users must comply with the requirements of the Data Protection Act (DPA) 1998, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.
- Users of the school's Computing systems and data must comply with the requirements of this policy.
- Users are responsible for notifying the Headteacher of any suspected or actual breach of IT security.
- The Headteacher shall inform both the ICO and Harrow Council if there are any losses of personal data.
- The school will work with the support teams of the school's MIS, financial and curriculum computer based systems to ensure the security of the data and safety of users.
- Users will be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities, to help safeguard systems and data.
- USO Nominated Contacts will use strong passwords when accessing or maintaining USO accounts.
- Appropriate procedures have been established to deal with the security implications of personnel changes.
- No personal data shall be taken from the school unless it is on encrypted media. This includes, but is not exclusive to, laptop computers, netbooks, external hard disks, USB memory sticks, Personal Digital Assistants (PDAs) and other portable digital technologies.
- Remote access to information and personal data shall only be provided through an encrypted link and users shall require a strong password that is renewed at least termly.
- Users shall not publish spread sheets, databases or other documents containing personal data on externally accessible web sites, including the MLE.

Physical Security:

- As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.
- Appropriate security arrangements will be applied during the removal of any ICT equipment from its normal location, taking into account the risks associated with the removal and the impact these risks might have.
- All school owned IT equipment and software will be recorded and an inventory maintained.
- Uninterruptible Power Supply (UPS) units will be used with servers and network cabinets.
- Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.
- Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and physically destroy disks and USB memory sticks.
- Users of the Computing systems will not:

- leave sensitive data on printers, computer monitors or desktops whilst away from their desk or computer;
- give out sensitive information unless the recipient is authorised to receive it;
- send sensitive/personal information via e-mail or post without suitable security measures being applied.

System Security:

• Users of the systems will **not**:
make, distribute or use unlicensed software or data;
make or send threatening, offensive or harassing messages;
create, possess or distribute obscene material;
reveal passwords to unauthorised persons;
create and use passwords that are obvious or guessable – their complexity should reflect the value and sensitivity of the systems and data.

• Passwords should be memorised –if they must be written down they should be kept in a secure location.

• Passwords shall be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.

• Users must ensure they have authorisation for private use of the school's computer facilities.

• Users who access personal data use a unique user ID and strong password that is renewed at least termly.

• Regular backups of MIS data, in accordance with the industry standard backup strategy used by the school's technical support company, are maintained and tested to ensure they enable data restoration in the event of system failure; copies are clearly marked and stored in a secure and fireproof location.

Virus Protection:

• The school should ensure current and up to date anti-virus software is applied to all school computing systems.

• Laptop users will ensure their virus protection is automatically updated at least weekly by connecting the laptop to the school's computer network (see also the school's Appropriate Use of Computing Systems Policy).

• Any suspected or actual virus infection must be reported immediately to the Computing Leader and that computer shall not be reconnected to the school network until the infection has been completely removed.

Disposal of Equipment:

• The School will ensure all personal data, records and software is obliterated from all hardware being disposed of. .

• The school will, as far as reasonably possible, ensure that any software remaining on a PC being relinquished for reuse is legitimate; care will be taken to avoid infringing software and data copyright and licensing restrictions by inadvertently supplying unlicensed copies of software.

- The School shall ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.

Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaints procedure.

Complaints which are not appropriate to be dealt with through the school's complaints procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact the Headteacher.

Further advice and information can be obtained from the Information Commissioner's Office, https://ico.org.uk or telephone 0303 123 1113.

Policy Review Schedule
Reviewed and amended at: **Full Governing Body: 2.2.17**
Next Review: February 2018 (in light of new Data Protection Act)