Priory Junior School

Data Protection Policy

The school collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the school in order provide education and associated functions. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Education Authorities (LEAs), government agencies and other bodies.

This policy is intended to ensure that personal information must be dealt with properly 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 used, recorded and stored and whether it is held in paper files or electronically.

Principles as laid down in the 1998 Data Protection Act must be followed at all times:

1. Data must be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specific and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose(s) 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 1998 Data Protection Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. At Priory Junior School, the Information Asset Owner is the Headteacher.

The role of an IAO is to understand:

- what information is held, and for what purposes
- what information needs to be protected (e.g. any data that can be linked to an individual, pupil or staff etc including UPN, teacher DCSF number etc)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

Data Gathering

All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act.

Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

Data Storage

Personal data will be stored in a secure and safe manner. Electronic data will be protected by standard password and firewall systems operated by the school.

Computer workstations in administrative areas will be positioned so that they are not easily visible to casual observers waiting either in the office or at the reception hatch. Screen savers are in place, and log outs are actioned, when admin staff are away from their desks.

Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.

Particular attention will be paid to the need for security of sensitive personal data.

School laptops are not currently encrypted. As such, no sensitive data should be stored on these. Staff should save documents on the school network staff share, or within Central Hosting whereby it can be accessed at home. The school provides all teachers with encrypted removable media – this is the only removable media permitted for use in school. The school intends to ensure all teacher's laptops are encrypted in the near future.

All media which is to be disposed of will be physically destroyed – these should be handed to the ICT subject leader, who will arrange for this to be done.

All users of the network have their own username and password, with appropriate permissions set for each group of users. The username and password must not be shared with anyone.
Passwords should be six characters or more, and consist of both alpha and numeric characters. To make the password stronger, it should have both upper and lower case.
Obvious passwords should be avoided (such as the cat's name or similar) and must be regularly changed – as prompted by the server.

The handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Data Checking

The school will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.

Any errors discovered will be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

Data Disclosures

Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.

When requests to disclose personal data are received by telephone it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.

If a personal request is made for personal data to be disclosed it is again the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.

Requests from parents or children for printed lists of the names of children in particular classes, which are frequently sought for parties/cards, should politely be refused as permission would be needed from all the data subjects contained in the list. (Note: A suggestion that the child makes a list of names when all the pupils are present in class will resolve the problem.)

Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

Routine consent issues will be incorporated into the school's pupil data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the school.

A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

Subject Access Requests

If the school receives a written request from a data subject to see any or all personal data that the school holds about them this should be treated as a Subject Access Request and the school will respond within the 40 calendar days deadline.

Informal requests to view or have copies of personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 10 day time limit.

This policy will be included in the *Staff Handbook*.

Data Protection statements will be included in the school prospectus and on any forms that are used to collect personal data. A Fair Processing Notice is issued to parents, and placed on the school website.

Retention of Records

Records are kept for as long as is necessary – for legal purposes, or information needs, and are then disposed of.

Financial records are kept for seven years.
Personnel records are kept for seven years after an employee leaves. Interview notes are kept for 6 months.

Pupil records are forwarded to the next school and are not kept. Copies of child protection records for a period of 12 months.

Personal assessment data is kept for 12 months and cohort assessment data is kept for 3 years.

Attendance data is kept for 3 years.

All documents are shredded when disposed of.

Electronic devices' drives are wiped clean when disposing of.

Revised February 2016