Primrose Hill Primary School

Data Protection Policy

June 2016

Review date: July 2018

DATA PROTECTION POLICY

At Primrose Hill, the Head Teacher, overseen by the Governing Board ensures that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Head Teacher and Governors of this school are intent to comply fully with the requirements and principles of the Data Protection Act 1998.

At Primrose Hill Primary School we intend that this policy will act as a guide for anyone working within the school who collects, manages, transfers or uses data about our learners, staff or other individuals during the course of their work.

Data Gathering

All personal data ('data which relates to a living individual who can be identified' e.g. address, telephone numbers, names, photographs) relating to staff, pupils or other people with whom the school has contact, whether held on computer or in paper files, is covered by the Act.

The personal data that will be protected will consist of any combination of data items that identifies an individual and gives specific information about them, their families or circumstances. This includes:

- Names
- Contact details
- Gender
- Date of birth
- Behaviour and assessment records

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. The School will check annually that the data collected is still adequate, relevant and not excessive in relation to the purpose for which the data is being held. Likewise data will not be kept for longer than is necessary. It is the duty of the school's Bursar to ensure that obsolete data is properly erased. Computer printouts, as well as source documents, are shredded before disposal.

Data Storage

All personal data will be stored in a secure and safe manner.
Electronic data will be protected by standard password systems operated by the school. No personal data (except names) will be held on teaching staff laptops or on staff USB devices.
Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process the data.

Data Checking

Data held will be as accurate as is reasonably possible. The school will issue regular reminders to staff and parents to ensure that data held is up-to-date and accurate.
If a parent ('a person having parental responsibility or care of a child', Education Act 1996) informs the school of a change in circumstances the computer record will be updated as soon as is possible.

Access to Records

Requests for access to personal data must be made in writing to the Head Teacher. It must include key information (e.g. full name, address and telephone number) in order for the school to verify the request.

Pupils, parents and staff may request access to the personal data held about them by the school. Provided that there is sufficient information to process the request this will be done within 40 days of the request. In the case of any written request from a parent regarding their own child's record, access to the record will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations. All personal data will be sent to the requesting person in a sealed envelope.

Data Disclosures

The School will, in general, only disclose data about individuals with their consent.
However, there are circumstances under which the Head Teacher may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Pupil data disclosed to authorise recipients related to education and administration for the school to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of the child's health, safety and welfare.
- Pupil data disclosed to parents in respect of their child's progress, achievements and attendance.
- Staff data disclosed to relevant authorities e.g. payroll and administration
- Disclosures to Police Officers if they are able to supply a written request which notifies the school of a specific and legitimate need to have access to specific personal data.

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

Data is not used in newsletters, websites or other media without prior consent. This includes the use of photographs. All parents are asked to give consent for this on admission to the school. A list of children who do not have permission is held by the Admin staff and circulated to staff annually.

Data and Computer Security (See appendix A)

The School undertakes to ensure the security of personal data by the following general methods (exact details, cannot, of course, be listed):

Physical Security

Appropriate building security measures are in place (lockable systems in the office). All printouts are locked in a secured place when not in use. Visitors to the school are required to sign in, to wear identification badges and, where appropriate, are accompanied.

Logical Security

Only authorised users are allowed to access the computer files and password changes are undertaken regularly. Computer files are backed up regularly.

Procedural Security

All staff are aware of their Data Protection responsibilities and the procedures in place for accessing personal data. These procedures are monitored and reviewed on a regular basis, especially if a security loophole becomes apparent.

Responsibility

Individual members of staff can be personally liable in law under the terms of Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorized use or disclosure of their data. A deliberate breach of this policy will be treated as a disciplinary matter.

Any queries or concerns about the security of data in school should, in the first instance, be referred to the Head Teacher.

Robin Warren
June 2016
Review Date: June 2018

DISSEMINATION OF THE POLICY

The policy will be given to all members of staff and copies will be available for parents.

PROCEDURES FOR MONITORING AND EVALUATION

The Head Teacher, members of the senior leadership team and members of the curriculum leadership team, will monitor the policy.

Good Practices for Working online

Do

- Make sure that you keep any computers that you own up to date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). Get advice from the school's IT technician or the EducationIT team at Camden if you need help.
- Only visit websites that are allowed by your organisation. Remember that Camden LEA may monitor and record (log) the websites you visit.
- Turn on relevant security warnings in your web browser (for example, the automatic phishing filter available in Internet Explorer and attack and forgery site warnings in Mozilla Firefox).
- Make sure that you only install software that the school's IT technician has checked and approved.
- Be wary of links to websites in emails, especially if the email is unsolicited.
- Only download files or programs from sources you trust. If in doubt, talk to the school's IT technician or the EducationIT team at Camden.
- Read the Primrose Hill esafety policy for the internet and its safe use and ensure that you follow it.

9.3 Email and messaging

Do

- Report any spam or phishing emails to the school's IT technician that are not blocked or filtered.
- Report phishing emails to the organisation they are supposedly from.
- Use your organisation's contacts or address book. This helps to stop email being sent to the wrong address.

Don't

- Click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on.
- Turn off any email security measures that the EducationIT team has put in place or recommended.
- Email sensitive information unless you know it is encrypted.
- Try to bypass your organisation's security measures to access your email off-site (for example, forwarding email to a personal account).
- Reply to chain emails.

9.4 Passwords

Do

- Follow your organisation's password policy.
- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers).
- Make your password easy to remember, but hard to guess, choose a password that is quick to type.
- Use a mnemonic (such as a rhyme, acronym or phrase) to help you remember your password
- Change your password(s) if you think someone may have found out what they are.

Don't

- Share your passwords with anyone else or write your passwords down.
- Use your work passwords for your own personal online accounts.
- Save passwords in web browsers if offered to do so.
- Use your username as a password.
- Use names as passwords.
- Email your password or share it in an instant message.

9.5 Laptops

Do

- Shut down your laptop using the 'Shut Down' or 'Turn Off' option.
- Try to prevent people from watching you enter passwords or view sensitive information.
- Turn off and store your laptop securely (if travelling, use your hotel's safe).
- Use a physical laptop lock if available to prevent theft.
- Lock your desktop when leaving your laptop unattended.
- Make sure your laptop is protected with encryption software.

Don't

- Store remote access tokens with your laptop.
- Leave your laptop unattended unless you trust the physical security in place.
- Use public wireless hotspots – they are not secure.
- Leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot.
- Let unauthorised people use your laptop.
- Use hibernate or standby.