Carlisle & Hampton Hill Federation

DATA PROTECTION POLICY

This policy was reviewed:	July 2018
This policy was ratified by Full Governing Body (if applicable):	July 2018
This policy will be reviewed again:	July 2019
Governor committee responsibility:	Achievement & Families Committee
Statutory Policy?:	Yes

This policy should be read in conjunction with the data privacy notices for pupils and staff, which will be reviewed by governors at the same time as this policy. In 2017/18 this policy was reviewed & approved by the FGB. This will be done by the Achievement & Families Committee in 2018/19

Data Protection Policy

Carlisle & Hampton Hill Federation is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors.

The Data Protection Act 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.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act. 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.

Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements. Carlisle Infant School and Hampton Hill Junior School are registered as Data Controllers with the Information Commissioners Office (ICO) detailing the information held and its use. Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The school collects a large amount of personal data every year, for example:

- pupil records
- parent/carer and other contacts details
- pupil medical information
- information about Special Educational Needs
- examination marks
- references
- Proof of right to work in the UK
- Proof of identity

In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

The Eight Data Protection Principles

The Act is based on eight data protection principles, or rules for 'good information handling'.

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.

Responsibilities of the school

The school must:

- Manage and process personal data properly
- Protect the individual's right to privacy
- Provide an individual with access to all personal data held on them.

The school is required to notify the Information Commissioner regarding the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website at the following link:

http://www.ico.org.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

Every member of staff that holds personal information has to comply with the Act when managing that information.

The school is committed to maintaining the eight principles at all times. This means that the school will:

- Inform data subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice, this is available on the Federation page of the website under Policies
- Check the quality and accuracy of the information held
- Apply the records management policies and procedures to ensure that information is not held longer than is necessary
- Ensure that when information is authorised for disposal it is done appropriately
- Ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- Only share personal information with others when it is necessary and legally appropriate to do so
- Set out clear procedures for responding to requests for access to personal information known as subject access request in the Data Protection Act (see link for guidance): https://ico.org.uk/fororganisations/guide-to-data-protection/principle-6-rights/subjectaccess-request/
- Train all staff so that they are aware of their responsibilities and of the schools relevant policies and procedures.

Personal and sensitive data

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely
- Personal information is not disclosed either orally or in writing or via web pages or by any other means, accidentally or otherwise, to any unauthorised third party
- Staff should note that unauthorised disclosure can be a disciplinary matter, and may be considered gross misconduct in some cases
- Staff should only use their designated email account to communicate about school. These are not secure accounts, and initials should be used to communicate about a specific child/ren not only in the body of emails, but in any attached documents.
- Data Controllers have access to the borough's secure document email system, and only these staff members can send and receive secure documents
- Personal information should:
    - Be kept in a filing cabinet, drawer, or safe in a secure office, or;
    - If it is computerised, be password protected both on a local hard drive and on a network drive that is regularly backed up; and
    - If a copy is kept on a USB stick or other removable storage media, that media must itself be password protected and/or kept in a filing cabinet, drawer, or safe.

Data Access Requests (Subject Access Requests)

All staff, parents and other users are entitled to:

- Know what information the school holds and processes about them or their child and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what the school is doing to comply with its obligations under the 1998 Act
- The school will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the school holds and processes about them, and the reasons for which they are processed
- All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing; which includes email, and be addressed to the Headteacher. The identity of the requestor must be established before the disclosure of any information. In the case of parent/carer requests, checks will be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:
    - Passport
    - Driving Licence
    - Utility Bill (with the current address)
    - Birth/Marriage Certificate
    - P45/P60
    - Credit Card/Mortgage Statement

    *Please note this list is not exhaustive

- The school may make a charge on each occasion that access is requested in order to meet the costs of providing the details of the information held
- The school aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

Location of information and data

Hard copy data, records and personal information are stored out of sight and in a locked cupboard. The only exceptions to this are medical information that may require immediate access during the school day and food allergy information (stored in the welfare room) that is required during lunchtimes (also stored in the kitchen).

Sensitive or personal information and data should not be removed from the school site, however, the school acknowledges that staff may need to transport data between the school and their home in order to access it for work in the evening and at weekends. This may also apply in cases where staff have off site meetings or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If they are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers
- If it is necessary to transport data away from the school, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only
- USB sticks that staff use must be password protected.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Retention of data

The school has a duty to retain some staff and pupil personal data for a period of time following their departure from the school, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time, this is outlined on our Retention of data schedule.

Monitoring and evaluation

This is ongoing; where any clarifications or actions are needed the policy will be amended at its next review.

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, www.ico.org.uk

Please follow this link to the ICO's website: (www.ico.org.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 1998.

Retention of Data Schedule

Pupils			
Basic File Description	**Data Protection Issues**	**Retention Period**	**Action at the end of the administrative life of the record**
Admission Details	Yes	Date of last entry in the book or file + 7 years	
Attendance Register	Yes	Date of register + 3 years	Secure disposal (electronic back-up copies should be permanently deleted at the same time)
Pupil files (hard copy)	Yes	Retain for the time the pupil is at school	Transfer to the school the pupil is going onto
Pupil files (electronic)	Yes	DOB + **18 years (to the end of school age)**	Secure complete deletion of file
Academic data (hard copy)	Yes	Retain for the time the pupil is at school	Transfer to the Junior School where the pupil is going
Academic data (electronic)	Yes	End of Key Stage + 3 years	Secure complete deletion of file
Parental permission slips for school trips where there has been no major incident	Yes	Conclusion of the trip	Secure disposal (shredding)
Parental permission slips for school trips where there has been a major incident	Yes	DOB of the pupil/s involved in the incident +25 years. The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils.	Secure disposal (shredding)
Walking Bus Registers (HHJS)	Yes	Date of register + 3 years. This takes into account the fact that if there is an incident requiring and	Secure disposal (electronic back-up copies should be destroyed at the same time)

		accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting.	
Safeguarding files (hard copy)	Yes	Retain for the time the pupil is at school	Transfer to the Junior School where the pupil is going
Special Educational Needs files (hard copy)	Yes	Retain for the time the pupil is at school	Transfer to the Junior School where the pupil is going

Staff
As per the Schools Financial Regulations and Standing orders (London Borough of Richmond). Copies available in school finance office.

Governors			
Minutes (principle set)	No	Permanent	Retain for 6 years from the date of meeting
Governor contact details (hard copy)	Yes	Duration of Appointment	Secure disposal (shredding)

Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer (DPO)

The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people.

The DPO will alert the Headteacher and the Chair of Governors

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned.

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored, on the school's computer system.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on the school's computer system.
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask LGFL to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted