LITTLE HEATH SCHOOL
DATA PROTECTION POLICY

Purpose and background

The handling of personal data is governed by legislation as set out in the European General Data Protection Regulation 2016 (GDPR) which was adopted into UK law by section 3 of the EU Withdrawal Act 2018 (UK GDPR) and the Data Protection Act 2018. Little Heath School has to ensure that it has robust systems and processes in place, as well as appropriately trained staff, to ensure that it complies with GDPR. GDPR covers all aspects of the handling of personal data including what personal data can be collected, how it must be stored, who can have access to it, how long it can be retained and how it should be disposed of.

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The lawful bases for processing personal data are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

d) **Vital interests:** the processing is necessary to protect someone's life.

e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

The GDPR applies to 'controllers' and 'processors'. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

The GDPR applies to 'personal data', meaning any information relating to an identifiable living person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier. Personal data that has been pseudonymised can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

The GDPR refers to 'sensitive personal data' as 'special categories of personal data'. This relates to information concerning a data subject's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences. The special categories specifically include genetic data and biometric data where processed to uniquely identify an individual.

Policy objectives

- to enable the school and individual members of staff to meet their legal and statutory duties in respect of data protection;

- to provide guidance for staff and governors as to how data protection matters are addressed within school.

Management of policy

School:	This policy is implemented and managed by the Headteacher, in consultation with the Data Officer.
Governing Body:	The Governors' Finance and Resources Committee reviews this policy on an annual basis and recommends amendments to the Governing Body for final decision.
Approval:	Approved by the Full Governing Body on 10th July 2023
Next review due:	July 2024

Associated policies

Freedom of Information Policy; Records Management and Retention Policy.

Practice and procedures

The Governing Body has adopted the West Berkshire Model Data Protection Policy for Schools. This policy recognises that all members of the school community have a role to play in effectively managing data protection. It is essential that this policy is brought to the attention of all existing staff, and that they are informed of any significant revisions to it. This policy must also form part of the induction process for all new staff.

Associated documents

Data Protection Act 2018
General Data Protection Regulation 2016

Appendices

Appendix 1: WBC Data Protection Model Policy for Schools
Appendix 2: Data Breach Procedure
Appendix 3: Little Heath School Privacy Notices
Appendix 4: Biometric Consent Form

Appendix 1: WBC Data Protection Model Policy
Aims & Objectives

The aim of this policy is to provide a set of guidelines to enable all members of staff to understand:

- The law regarding personal data;
- The importance of Personal Data governance;
- How personal data should be processed, stored, archived and deleted/destroyed;
- How staff, parents and pupils can access personal data;
- Examples of good practices.

The objective of the policy is to ensure that Little Heath School acts within the requirements of the Data Protection Act 2018 and General Data Protection Regulation (GDPR) when retaining and storing personal data, and when making it available to individuals.

Data Protection – the law

- Under the Data Protection Act 2018, and other regulating Acts, access to their own personal data is a statutory right for pupils (if they are of an age to understand the data they request) and parents (as defined in the Education Act 1996) may also request access to their child's educational records.
- School staff have a right of access to personal data on themselves.
- Anyone has the right to question and correct inaccurate data, but this must be matters of fact, not opinions.
- Personal data should always be kept securely and protected by passwords if it is electronic, and processing of the data should only be by those authorised to do so – maintaining privacy is the school's responsibility.
- The law also provides that personal data should not be kept longer than is required.
- Third party data (information about someone other than the requesting individual) should in general only be provided with their permission.
- The Headteacher is the named person with overall responsibility for personal data within Little Heath School.

The importance of Personal Data governance

The smooth running of a school involves a high level of trust amongst all members of the school community. When large amounts of personal data are being stored in IT and paper -based systems set up by the school, data protection is an important responsibility for all members of staff.

There are many benefits: - imagine the time we can all save from sharing a well organised archive where teachers can search for pupil data easily; imagine the reputational damage the school would suffer from when ransomware managed to get onto our school system and we have to pay a large sum of money or suffer from days of system outage?

Fair processing of personal data: data which may be shared

Schools, local education authorities and the Department for Education (DfE) all hold information on pupils in order to run the education system, and in doing so have to follow the Data Protection and related Acts. This means, among other things that the data held about pupils must only be used for specific purposes allowed by law. The school has Fair Processing or Privacy Notices which explain how personal data is used and with whom it will be shared. Examples of these Notices are published on the school's website and forms appendix 3 of this policy.

Processing, storing, archiving and deleting personal data: guidance

- Personal data and school records about pupils are confidential to the child. The information can be shared appropriately within the professional working of the school to enable the school to make the best educational provision for the child. The law permits such information to be shared with other educational establishments when pupils change schools.
- School records for a child are kept for seven years after the child leaves the school unless subject to legal hold and or for children with special educational needs.
- Data on staff is sensitive information and confidential to the individual. It is only shared, where appropriate, at the discretion of the Head Teacher and with the knowledge, and if possible the agreement of the staff member concerned. This includes data on school-provided e-mail system.
- Employment records form part of a staff member's permanent record. Because there are specific legislative issues connected with these (salary and pension details etc.) these records should be retained as set out by the Local Authority
- Interview records, CVs and application forms for unsuccessful applicants are kept for 6 months.
- All formal complaints made to the Head Teacher or School Governors will be kept for at least seven years in confidential files, with any documents on the outcome of such complaints. Individuals concerned in such complaints may have access to such files subject to data protection and to legal professional privilege in the event of a court case.
- All members of staff should only access school-provided systems (including email) up to the last day of employment.

Accessing personal data: guidance

- A child can request access to his/her own data. The request is not charged and does not have to be in writing. The staff will judge whether the request is in the child's best interests, and that the child will understand the information provided. They may also wish to consider whether the request has been made under coercion. All decisions should be documented.
- A parent can request access to or a copy of their child's school records and other information held about their child. The request must be made in writing. There is no charge for such requests on behalf of the child, but there may be an agreed charge for photocopying existing non-digital records. Staff should check, if a request for information is made by a parent, that no other legal obstruction (for example, a court order limiting an individual's exercise of parental responsibility) is in force.
- Parents should note that all rights under the Data Protection Act to do with information about their child rest with the child as soon as they are old enough to understand these rights. This will vary from one child to another, but, as a broad guide, it is reckoned that most

children will have a sufficient understanding by the age of 12. Parents are encouraged to discuss and explain any request for information with their child if they are aged 12 or over.

- Separately from the Data Protection Act, The Education (Pupil Information England) Regulations 2005 provide a pupil's parent (regardless of the age of the pupil) with the right to view, or to have a copy of, their child's educational record at the school. Parents who wish to exercise this right must apply to the school in writing.
- For educational records (unlike other personal data; see below) access must be provided within 15 school days, and if copies are requested, these must be supplied within 15 school days of payment of the cost of copying.
- A member of staff can request access to their own records at no charge, but the request must be made in writing. The member of staff has the right to see their own records, and to ask for copies of the records. There is no charge for copies of records.
- GDPR requires that all requests for personal information are dealt with within 1 month of receipt except requests for educational records (see above) or with agreement with the Data Subject. All requests will be acknowledged in writing, and access to records will be arranged as soon as possible. If awaiting third party consents, the school will arrange access to those documents already available, and notify the individual that other documents may be made available later.
- In all cases, should third party information (information about another individual) be included in the information the staff will try to obtain permission from the third party to show this information to the applicant. If third party permission is not obtained the person with overall responsibility should consider whether the information can still be released.
- Personal data should always be of direct relevance to the person requesting the data. A document discussing more general concerns may not be defined as personal data.
- Under the Freedom of Information Act definition, a request for personal information can include unstructured as well as structured records – for example, letters, emails etc. not kept within an individual's personal files, or filed by their name, but still directly relevant to them. If these would form part of a wider record it is advisable to file these within structured records as a matter of course and to avoid excessive administrative work in the future.
- Anyone who requests to see their personal data has the right to question the accuracy of matters of fact within the data, and to ask to have inaccurate information deleted or changed. They may also question opinions, and their comments will be recorded, but opinions do not need to be deleted or changed as a part of this process.
- The school will document all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes (letter requesting changes etc.) This will enable staff to deal with a complaint if one is made in relation to the request.

Examples of good practices

- Only school-provided data storage (which are centrally archived/encrypted) should be used to store work-related personal data. No USB pen is to be used for storing personal data.
- Avoid using unknown supplier of Wi-Fi services for work activities which involve personal data.
- Work out how to change your password without the need for help, before you need to do so to address issues.
- Do not open uninvited e-mail from unrecognised source – check its source with a phone call or delete the mail item without opening any attachment / click on any links.
- Only use computers which have operational anti-virus software.

- Use a secure e-mail tool where available by default for all communication involving personal data.
- Avoid using a person's full name in an e-mail subject line, nor as a filename – as soon as you do, they are subject to data access request.
- Look out for unexpected behaviour of your computer – if in doubt, check with a colleague.
- Log queries as questions for your next CPD – everything has an explanation.
- Work to separate (storage of) personal and non-personal data as and when data are being worked on.
- Get to know the steps you need to follow when personal data is lost / leaked to the open world.
- Practice what we preach – for example, never share a password, however inconvenient it might be at the time. Children would pick up good practices from us – it is their future we are working to safeguard.

Appendix 2: Data Breach Procedure

Little Heath School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Little Heath School and all school staff, Governors, volunteers and contractors, referred to herein after in this appendix as 'staff'.

This breach procedure sets out the course of action to be followed by all staff at Little Heath School if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
   a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   c) describe the likely consequences of the personal data breach;
   d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Types of Breach

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a Data Breach

In the event that the School identifies or is notified of a personal data breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the Headteacher or, in their absence, either the Deputy Head Teacher and/or the School's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Headteacher/DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff.

3. The Headteacher/DPO (or nominated representative) must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

4. The Headteacher/DPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the WBC Legal Services should be obtained.

5. The Headteacher/DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. Contacting the WBC Press Office, so that they can be prepared to handle any press enquiries.

c. The use of back-ups to restore lost/damaged/stolen data.

d. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

e. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Headteacher/DPO (or nominated representative) to fully investigate the breach. The Headteacher/DPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- Quantity of data;
- What type of people have been affected (pupils, staff members, suppliers etc.) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Headteacher/DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the Headteacher/DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the

response to it. It should be reported to the next available Senior Leadership Team meeting and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these rights. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with HR for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Headteacher/DPO should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Headteacher.

Appendix 3: Little Heath School Privacy Notices

Privacy Notice (How we use pupil information)

The categories of pupil information that we process include:

- personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- characteristics (such as ethnicity, language, and free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- special educational needs (including the needs and ranking)
- medical and administration (such as doctors' information, child health, dental health, allergies, medication and dietary requirements)
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment (such as post 16 courses enrolled for and any relevant results)
- behavioural information (such as exclusions and any relevant alternative provision put in place)
- catering and free school meal management (such as allergies and special dietary requirements)
- trips and activities (such as doctors' information and health information)
- identity management/authentication (such as biometric information and photographs)
- CCTV images captured in school

Why we collect and use pupil information

The personal data collected is essential, in order for the school to fulfil their official functions and meet legal requirements. We collect and use pupil information, for the following purposes:

a) to support pupil learning and wellbeing
b) to monitor and report on pupil attainment progress
c) to provide appropriate pastoral care
d) to assess the quality of our services
e) to keep children safe (food allergies, or emergency contact details)
f) to meet the statutory duties placed upon us for DfE data collections

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing pupil information are: for the purposes of (a), (b), (c) & (d) in accordance with the legal basis of Public task: collecting the data is necessary to perform tasks that schools are required to perform as part of their statutory function

- for the purposes of (e) in accordance with the legal basis of Vital interests: to keep children safe (food allergies, or medical conditions)
- for the purposes of (f) in accordance with the legal basis of Legal obligation:
    - data collected for DfE census information
    - Section 537A of the Education Act 1996
    - the Education Act 1996 s29(3)
    - the Education (School Performance Information) (England) Regulations 2007
    - regulations 5 and 8 School Information (England) Regulations 2008
    - the Education (Pupil Registration) (England) (Amendment) Regulations 2013

In addition, concerning any special category data: conditions a, b, c and d of GDPR - Article 9

How we collect pupil information

We collect pupil information via the SIMS Parent App or data collection sheets each academic year. In addition, when a child joins us from another school we are sent a secure file containing relevant information.

During the school year, additional information may be collected via a medical and consent form for school trips.

Pupil data is essential for the schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

How we store pupil data

We hold pupil data securely for the set amount of time shown in our data retention schedule which forms part of our Records Management and Retention Policy.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupils attend after leaving us
- our local authority
- youth support services (pupils aged 13+)
- the Department for Education (DfE)
- secure on-line learning platforms
- secure on-line payment system
- canteen and library biometric system supplier
- school nurse

Why we regularly share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

Youth support services

Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to the child's name, address and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / pupil once they reach the age 16.

Pupils aged 16+

We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19-year olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under:

- Section 537A of the Education Act 1996
- the Education Act 1996 s29(3)
- the Education (School Performance Information) (England) Regulations 2007
- regulations 5 and 8 School Information (England) Regulations 2008
- the Education (Pupil Registration) (England) (Amendment) Regulations 2013

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework. For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Data Protection Officer, Little Heath School email dpo@littleheath.org.uk.

You also have the right to:
- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact: Data Protection Officer, Little Heath School email dpo@littleheath.org.uk.

How Government uses your data

The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures) supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).
The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.
It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.
To find out more about the NPD, go to
https://www.gov.uk/government/publications/national-pupil-database-user-guideand-supporting-information

Sharing by the Department

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit:

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares

To contact DfE: https://www.gov.uk/contact-dfe

Privacy Notice (How we use workforce information)

The categories of school information that we process include:

- personal information (such as name, address, employee or teacher number, national insurance number)
- characteristics information (such as gender, age, ethnic group)
- contract information (such as start date, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- relevant medical information (such as allergies)
- CCTV images captured in school

Why we collect and use workforce information

We use workforce data to:

a) enable the development of a comprehensive picture of the workforce and how it is deployed
b) inform the development of recruitment and retention policies
c) enable individuals to be paid
d) carry out employment checks e.g. right to work in the UK, DBS
e) keep staff safe (food allergies, medical conditions)
f) meet the statutory duties placed upon us

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing workforce information for general purposes are:

- for the purposes of (a) and (b) in accordance with the legal basis of Public task; collecting the data is necessary to perform tasks that schools are required to perform as part of their statutory functions
- for the purposes of (c) and (d) in accordance with the legal basis of Contract; the processing is necessary for a contract the school has with the individual or because they have asked the school to take specific steps before entering in to a contract
- for the purpose of (e) in accordance with the legal basis of Vital interest
- for the purpose of (f) in accordance with the legal basis of Legal Obligation; data collected for DfE workforce information under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

  In addition, concerning any special category data:

- conditions a, b, c, d and h of GDPR - Article 9

Collecting workforce information

We collect personal information via our job application processed, staff contract forms and annual staff data collection sheets.
Workforce data is essential for the school's / local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information

We hold data securely for the set amount of time shown in our data retention schedule the details of which are set out in the school's Records Management and Retention Policy.

Who we share workforce information with

We routinely share this information with:

- our local authority
- the Department for Education (DfE)

Why we share school workforce information

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children and young people with the Department for Education (DfE).

We are required to share information about our school employees with the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Data Protection Officer, Little Heath School, email dpo@littleheath.org.uk.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact: Data Protection Officer, Little Heath School, email dpo@littleheath.org.uk

How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Sharing by the Department

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

To contact the department: https://www.gov.uk/contact-dfe

Privacy Notice (How we use visitor information)

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data. This privacy notice explains how we collect, store and use personal data about visitors to the school, in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. We, Little Heath School, are the 'data controller' for the purposes of data protection law. This means that we are responsible for deciding how we hold and use personal information about you.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Name
- Contact details
- DBS clearance
- Information relating to your visit, e.g. your organisation name, arrival and departure time, car registration number
- Photographs for identification purposes for the duration of your visit
- CCTV images captured in school
- Information about any access arrangements you may need

Why we use this data

- Identify you and keep you safe while on the school site
- Keep pupils and staff safe
- Maintain accurate records of visits to the school
- Provide appropriate access arrangements

Our lawful basis for using this data

We only collect and use your personal data when the law allows us to. Most commonly, we process it where we need to comply with our legal obligation to keep our pupils and staff safe while on the school premises. Less commonly, we may also process your personal data in situations where:

- We need it to perform an official task in the public interest
- We have obtained consent to use it in a certain way
- We need to protect someone's vital interests (save your life, or someone else's)

Collecting this information

Some of the information we collect from you is mandatory, and in some cases, you can choose whether or not to provide the information to us. Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice. We will only collect the data that we need in order to fulfil our purposes, which are set out above.

How we store this data

We will keep your personal data while you are visiting our school. We may also keep it beyond this, if necessary, to comply with our legal obligations. Information and Records Management Society's toolkit for schools sets out how long we keep information about visitors. We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We will dispose of your personal data securely when we no longer need it.

Data sharing

We do not share information about visitors with any third party without consent unless the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about visitors with:

- Our local authority – to meet our legal obligations to share certain information with it, such as where the visitor information is relevant to a safeguarding concern
- The Department for Education
- Our regulator [specify as appropriate, e.g. Ofsted, Independent Schools Inspectorate]
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Health authorities
- Security organisations
- Health and social welfare organisations
- Police forces, courts, tribunals
- Professional bodies
- The organisation/company you are representing

Your rights

- Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:
- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict its processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer (details below).

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please email our data protection officer: dpo@littleheath.org.uk This notice is based on the Department for Education's model privacy notices, amended for visitors and to reflect the way we use data in this school. We regularly review and, where necessary, update our Privacy Notices. Please refer to our website for the latest version.

Appendix 4: Biometric Consent Form

Please complete this form and return to the school office

Biometric Consent

Little Heath School uses a cashless catering system which uses biometric data. Simply stated, your child`s finger is registered which is translated to an alpha numeric number, the image is then discarded. When used this will enter the student into a system program and identify them by a number, we also use the biometric system in the library. We require parental consent to record your child`s biometric information. This data will only be used within the school and will be deleted when your child leaves Little Heath. If you require more information please do not hesitate to contact the school.

Conditions of use:

- The school will collect biometric data responsibly and keep it secure in compliance with General Data Protection Regulation (GDPR).
- The school will not use biometric information for any purpose other than the school systems.
- The school will only share this information with the suppliers of our biometric information systems and will not unlawfully disclose it to any other person.
- The school will ensure that the suppliers of our biometric information systems meet GDPR regulations.

I confirm that I have read and understood the information above and my decision in regard to biometric recognition is indicated below. *(Please note that if consent is given you have the right to withdraw it at any time in the future. Any such request should be submitted in writing to the main school office).*

Student name	
I consent for my child's biometric image to be used as stated above	YES / NO
Parent / Carer name	
Parent / Carer signature	
Student signature	
Date	