All Mulberry House School policies are always to be read and considered in conjunction with Equal Opportunities, Race Equality and Inclusion policies.

MULBERRY HOUSE SCHOOL
DATA PROTECTION POLICY

This Policy of Mulberry House School applies to all sections of the school including the Early Years Foundation Stage. Please read this policy in conjunction with the E-safety policy and Confidentiality policy.

The School will comply with:

- The terms of the 1998 Data Protection Act, and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.
- The Privacy and Electronics Communication Regulations 2011.
- The Protection of Freedoms Act 2012.
- Information and guidance displayed on the Information Commissioner's website www.ico.gov.uk

Statement of Intent

The Proprietor, Director and Headteacher have overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Proprietor, Director and the Headteacher of the School intend to comply fully with the requirements and principles of the Data Protection Act 1984 and the Data Protection Act 1988. All of the staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

Types of Personal Data Processed by the School

The school may process a wide range of personal data about individuals including current, past and prospective pupils and their parents as part of its operation, including by way of example:

- names, addresses, telephone numbers, e-mail addresses and other contact details;
- bank details and other financial information, e.g. about parents who pay fees to the school or payroll details for members of staff;
- past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs);
- where appropriate, information about individuals' health, and contact details for their next of kin;
- references given or received by the school about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils; and
- images of pupils (and occasionally other individuals) engaging in school activities, and images captured by the school's CCTV system (in accordance with the school's E-Safety policy);

Generally, the school receives personal data from the individual directly (or, in the case of pupils, from parents). However, in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual), or collected from publicly available resources.

Sensitive Personal Data

The school may, from time to time, need to process "sensitive personal data" regarding individuals. Sensitive personal data includes information about an individual's physical or mental health, race or ethnic origin, political and religious beliefs. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the school with the explicit consent of the appropriate individual, or as otherwise permitted by the Act.

Personal Data

Use of Personal Data by the School:

The school will use (and where appropriate share with third parties) personal data about individuals for a number of purposes as part of its operations, including as follows:

- For the purposes of pupil selection and to confirm the identity of prospective pupils and their parents;
- To provide education services (including SEN), career services, and extra-curricular activities to pupils; monitoring pupils' progress and educational needs; and maintaining relationships with alumni and the school community;
- For the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the school's performance;
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend;
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the school;
- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;
- To monitor (as appropriate) use of the school's IT and communications systems in accordance with the school's IT acceptable use policies;
- To make use of photographic images of pupils in school publications, on the school website and (where appropriate) on the school's social media channels in accordance with the school's policy on taking, storing and using images of children;
- For security purposes, and for regulatory and legal purposes (for example child protection and health and safety) and to comply with its legal obligations; and
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

Fair Obtaining and Processing

The Mulberry House School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subject’s right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting will explain the issues before obtaining the information.

"processing" means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.

"data subject" means an individual who is the subject of personal data or the person to whom the information relates.

"personal data" means data, which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.

"parent" has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child.

Data Integrity

The School undertakes to ensure data integrity by the following methods:

Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances, their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects annually so they can check its accuracy and make any amendments. A copy is kept on file for the academic year and then shredded. The office retains a copy of the data for the full time that the child is at the school. These documents are then archived.

Where a data subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Headteacher for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the School will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data. *(The Headteacher will arrange an annual check on records for irrelevant data and is responsible for what must be deleted).*

Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Bursar to ensure that obsolete data are properly erased.

Subject Access

The Data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves, it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the School's policy is that:

- Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.

- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.

- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

Processing Subject Access Requests

Requests for access must be made in writing.

Pupils, parents or staff may ask for a Data Subject Access form, to be found below. Completed forms should be submitted to Jay Harley (Bursar and Data Manager). Provided that there is sufficient information to process the request, an entry will be made in the Accident/Incident/Injury Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (eg Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

Note: 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.

Authorised Disclosures

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

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.

- Pupil data disclosed to authorised recipients in respect of their child's welfare, health and, safety.

- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.

- Staff data disclosed to relevant authorities eg in respect of payroll and administrative matters.

- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of contracting companies, are contractually bound not to disclose personal data.

- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the School by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the School who **needs to know** the information in order to do their work. The School will not disclose anything on pupils' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything which suggests that they are, or have been, either the subject of or at risk of child abuse.

  A **"legal disclosure"** is the release of personal information, in what ever form, to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

  An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School's registered purposes.

Data and Computer Security

The Mulberry House School undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

Physical Security

Appropriate building security measures are in place, such as alarms, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the IT office and server rooms. Disks, tapes, other Data storage devices and printouts are locked away securely when not in use. Visitors to the School are required to sign in and out, to wear identification badges whilst in the School and are, where appropriate, accompanied.

Logical Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up regularly.

Procedural Security

In order to be given authorised access to the computer all staff will be required to read the policy and have training in their Data Protection obligations and their knowledge updated as necessary. Training will be

provided as part of their induction. Computer printouts as well as source documents are shredded before disposal.

Overall this policy for data is determined by The Headteacher and is monitored and reviewed annually, and when/if a security loophole or breach becomes apparent.

Any queries or concerns about security of data in the School should in the first instance be referred to Jay Harley, Data Manager.

Further guidance on the School's Security arrangements may be obtained from the Bursar or be found as appropriate in the E-Safety Policy.

Taking Photographs at School

The Data Protection Act is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos. Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.

- Photos taken for official school use may be covered by the Act and pupils and students should be advised why they are being taken.

Personal use:

- A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply.
- Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply.

Official school use:

- Photographs of pupils or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the Act will apply.
- A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the Act as long as the children and/or their guardians are aware this is happening and the context in which the photo will be used. Permission is sought through the Parental contract, at which time parents are given the option to opt out. Information on who might have opted out is held by the office. Staff may ask for details of who is on the list at any time.

Media use:

- A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act.

Pupils

Pupils' Rights

The rights under the Act belong to the individual to whom the data relates. However, the school will in most cases rely on parental consent to process personal data relating to pupils (if consent is required under the Act) unless, given the nature of the processing in question, and the pupil's age and understanding, it is more appropriate to rely on the pupil's consent. Parents should be aware that in such situations they

may not be consulted. In general, the school will assume that pupils consent to the disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the school's opinion, there is a good reason to do otherwise. However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the school will maintain confidentiality unless, in the school's opinion, there is a good reason to do otherwise; for example, where the school believes disclosure will be in the best interests of the pupil or other pupils. Pupils are required to respect the personal data and privacy of others, and to comply with the school's IT Acceptable Use Policy and the school rules.

Staff

The Data Protection Code of Conduct

The following Code must be adhered to at all times:

- Staff should only ever share information on a “need to know basis”.
- Data protection should never be used as an excuse for not sharing information where necessary. The welfare of the child is paramount.
- Seniority does not give an automatic right to information.
- All emails are disclosable, less a few exemptions.
- Only keep data for as long as is necessary.

Confidentiality

Any School information/records including details of pupils, parents and employees whether actual, potential or past, other than those contained in authorised and publicly available documents, must be kept confidential unless the School's prior written consent has been obtained. This requirement exists both during and after employment. In particular, such information for the benefit of any future employer.

Off Site Access

See also the School’s E-Safety Policy which states that: “The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. This is in relation to data belonging to all members of the school community. As such, no member of staff is permitted to remove sensitive personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Headteacher. Where a member of staff is permitted to download data off site it will need to be password protected.”

There is one exception where prior approval is not required:

- For pupils on residential trips, medical information and other relevant information (e.g. passport details) may be taken off site by the trip leader.

What to do in the Event of a Suspected Data Breach

A personal data breach is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service”. A personal data breach may mean that someone other than the school gets unauthorised access to personal data. But a personal data breach can also occur if there is unauthorised access within the school or if a member of staff accidentally alters or deletes personal data.

In the event of a breach, the member of staff must notify the Headteacher and Bursar within 24 hours of becoming aware of the breach and fill in the data breach

form attached to this policy.
This notification must include at least:
- your name and contact details;
- the date and time of the breach (or an estimate);
- the date and time you detected it;
- basic information about the type of breach; and
- basic information about the personal data concerned.

The Headteacher will then make a judgement on the best course of action which is likely to include notifying the Proprietor and Director, plus the Designated Safeguarding Lead in the event that the data breach includes pupils' details, as appropriate.

Data Retention and Storage Guidelines
In these guidelines, "record" means any document or item of data which contains evidence or information relating to the school, its staff, parents or pupils. Some of this material will contain personal data of individuals as defined in the Act: but not all. Many, if not most, new and recent records will be created, received and stored electronically. Others (such as Certificates, Registers, or older records) will be original paper documents. The format of the record is less important than its contents and the purpose for keeping it.

Storage of Records:
Digital records.
Digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive data - or any large quantity of data - should as a minimum be password protected and held on a limited number of devices only, with passwords provided on a need-to-know basis and regularly changed. Emails (whether they are retained electronically or printed out as part of a paper file) are also "records" and may be particularly important: whether as disclosable documents in any litigation, or as representing personal data of the sender (or subject) for data protection/data privacy purposes. Again, however, the format is secondary to the content and the purpose of keeping the document as a record. It is important that all staff bear in mind, when creating documents and records of any sort (and particularly email), that at some point in the future those documents and records could be disclosed - whether as a result of litigation or investigation, or because of a subject access request under the Act.

Paper records.
Paper records should be stored in dry, cool, reasonably ventilated storage areas. Under the Act, paper records are only classed as personal data if held in a "relevant filing system". This means organised, and/or indexed, such that specific categories of personal information relating to a certain individual are readily accessible, and thus searchable as a digital database might be. By way of example, an alphabetical personnel file split into marked dividers will likely fall under this category: but a merely chronological file of correspondence may well not. However, when personal information is contained on print-outs taken from electronic files, this data has already been processed by the school and falls under the Act.

Archiving and the Destruction or Erasure of Records.
Staff given specific responsibility for the management of records must ensure, as a minimum, the following:

- That records - whether electronic or hard copy - are stored securely as above, including if possible with encryption, so that access is available only to authorised persons and the records themselves are available when required

and (where necessary) searchable;

- That important records, and large or sensitive personal databases, are not taken home or - in respect of digital data - carried or kept on portable devices (whether CDs or data sticks, or mobiles and handheld electronic tablets) unless absolutely necessary, in which case it should be subject to a risk assessment and in line with the E-Safety policy (therefore written permission requested in advance less the exemptions listed);
- That questions of back up or migration are likewise approached in line with general school policy (such as professional storage solutions or IT systems) and not individual ad hoc action;
- That arrangements with external storage providers - whether physical or electronic (in any form, but most particularly "cloud-based" storage) - are supported by robust contractual arrangements providing for security and access;
- That reviews are conducted on a regular basis, in line with the guidance below, to ensure that all information being kept is still relevant and - in the case of personal data - necessary for the purposes for which it is held (and if so, that it is accurate and up-to-date); and
- That all destruction or permanent erasure of records, if undertaken by a third party, is carried out securely - with no risk of the re-use or disclosure, or re-construction, of any records or information contained in them. For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. Paper records should be shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed. Where third party disposal experts are used they should ideally be supervised but, in any event, under adequate contractual obligations to the school to process and dispose of the information securely.

Table of Suggested Retention Periods

Type of Record/Document	Suggested* Retention Period
SCHOOL-SPECIFIC RECORDS	
• Registration documents of School	Permanent (or until closure of the school)
• Attendance Register	6 years from last date of entry, then archive.
• Minutes of Governors' meetings	6 years from date of meeting
• Annual curriculum	From end of year: 3 years (or 1 year for other class records: eg marks / timetables / assignments)
INDIVIDUAL PUPIL RECORDS	NB - this will generally be personal data
• Admissions: application forms, assessments, records of decisions	Up to 7 years from pupil leaving school (if admitted); up to 7 years from decision otherwise.
• Examination results (external or internal)	7 years from pupil leaving school
• Pupil file including pupil reports	25 years from date of birth
• Pupil medical records	25 years from date of birth
• Pupil performance records	7 years from pupil leaving school (unless there is good reason to consider they may be applicable evidence in a medical, negligence or abuse claim).
• Special educational needs records (to be risk assessed individually)	Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)
RECORDS RELATING TO EVENTS (such as guest lists, financial information (eg Credit Card details etc.)	For no longer than is necessary to conduct the event and to provide management information for future events.
SAFEGUARDING	
• Policies and procedures	Keep a permanent record of historic policies
• DBS disclosure certificates (potentially sensitive personal data & must be secure)	No longer than 6 months from decision on recruitment, unless DBS specifically consulted. (but keep a record of the fact that checks were undertaken, if not the information itself).
-	
-	
• Incident reporting	Where an issue or concern relating to a member of staff and the safeguarding of children has been identified, records of any concerns, suspicions or investigations will be kept for 75 years. Allegations which prove to be malicious will not be kept as part of the personnel record. Limitation periods can be dis-applied in criminal and civil abuse cases; to be weighed against rights under the DPA and insurers' requirements.
CORPORATE RECORDS (where applicable)	e.g. where schools have trading arms
• Certificates of Incorporation	Permanent (or until dissolution of the company)
• Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum - 10 years

Type of Record/Document	Suggested* Retention Period
• Shareholder resolutions	Minimum - 10 years
• Register of Members/Shareholders	Permanent (minimum 10 years for ex-members/shareholders)
• Annual reports	Minimum - 6 years
ACCOUNTING RECORDS** • Accounting records (normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state) [NB specific ambit to be advised by an accountancy expert]	Minimum - 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place Internationally: can be up to 20 years depending on local legal/accountancy requirements
• Tax returns	Minimum - 7 years
• VAT returns	Minimum - 7 years
• Budget and internal financial reports	Minimum - 3 years
CONTRACTS AND AGREEMENTS • Signed or final/concluded agreements (plus any signed or final/concluded variations or amendments)	Minimum - 7 years from completion of contractual obligations or term of agreement, whichever is the later
• Deeds (or contracts under seal)	Minimum - 13 years from completion of contractual obligation or term of agreement
INTELLECTUAL PROPERTY RECORDS • Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years.
• Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
• IP / IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; co-existence agreements; consents)	Minimum - 7 years from completion of contractual obligation concerned or term of agreement
INSURANCE RECORDS Insurance policies (will vary - private, public, professional indemnity)	Permanent
Correspondence related to claims/ renewals/ notification re: insurance	Permanent
PENSION RECORDS Pension records for pension funds managed by the school for support staff	Permanent
ENVIRONMENTAL & HEALTH RECORDS Maintenance logs Accidents to children***	10 years from date of last entry 25 years from birth

Type of Record/Document	Suggested* Retention Period
Accident at work records (staff)***	Minimum - 4 years from date of accident, but review case-by-case where possible
Staff use of hazardous substances*** Risk assessments*** (carried out in respect of above)	Minimum - 7 years from end of date of use 7 years from completion of relevant project, incident, event or activity.

Standard Recommended Employment Records Retention Periods

Type of employment record	Statutory or Code of Practice reference	Format and location	Retention period or recommendation
Job applications and interview records of unsuccessful candidates	The Information Commissioner: Employment Practices Code	Paper or electronic	A short period, of c6 months after notifying unsuccessful candidates.
Personnel and training records	N/A	Paper or electronic	While employment continues and up to six years after employment ceases
Written particulars of employment, contracts of employment, and changes to terms and conditions	N/A	Paper or electronic	While employment continues and up to six years after employment ceases
Working time opt-out forms	Working Time Regulations (WTR)	Paper or electronic originals are not required by the *WTR*	Two years from the date on which they were entered into

Type of employment record	Statutory or Code of Practice reference	Format and location	Retention period or recommendation
Records to show compliance with the WTR	WTR	Paper or electronic	Two years after the relevant period
Annual leave records	N/A	Paper or electronic	Six years or possibly longer if leave can be carried over from year to year
Payroll and wage records for companies	Finance Act 1988	Paper or electronic	7 years from the financial year-end in which payments were made
PAYE (Pay As You Earn)	Income Tax Regulations 2003	Paper or electronic	7 years from the financial year-end in which payments were made
Maternity records	Statutory Maternity Pay Regulations 1986	Paper or electronic	7 years from the financial year-end in which payments were made
Sickness records required for the purposes of Statutory Sick Pay (SSP)	Statutory Sick Pay Regulations 1982	Paper or electronic	7 years from the financial year-end in which payments were made
Current bank details	N/A	Paper or electronic	No longer than necessary
Records of advances of loans to employees (now ceased)	N/A	Paper or electronic	While employment continues and up to six years after repayment
Death Benefit Nomination and Revocation Forms	N/A	Paper or electronic	Permanent during staff member's employment

Type of employment record	Statutory or Code of Practice reference	Format and location	Retention period or recommendation
Records in relation to hours worked and payments made to workers	National Minimum Wage legislation	Paper or electronic	7 years from the financial year-end in which payments were made
Consents for the processing of personal and sensitive data	DPA	Paper or electronic	For as long as the data is being processed and up to 6 years afterwards
Disclosure and Barring Service (DBS) (formerly Criminal Records Bureau (CRB)), checks and disclosures of criminal records forms	Information Commissioner's Employment Practices Code	Paper or electronic	Should be deleted following recruitment process unless assessed as relevant to ongoing employment relationship. Once the conviction is spent, should be deleted unless it is an excluded profession
Immigration checks	Immigration, Asylum and Nationality Act 2006	Paper or electronic	Two years after the termination of employment

CCTV Policy

The Mulberry House School has in place a closed circuit television ("CCTV") system to provide a safe and secure environment for students, staff, visitors, and to protect school property. This document sets out the accepted use and management of the CCTV system and images to ensure the School complies with the Data Protection Act, Human Rights Act 1998 (HRA) and other legislation. This policy has been produced in line with the Information Commissioner's CCTV Code of Practice and the Home Office Surveillance Camera Code of Practice.

The Purpose of CCTV

The School has installed a CCTV system to:

- Deter crime.
- Assist in prevention and detection of crime.
- Assist with the identification, apprehension and prosecution of offenders.
- Monitor security of our buildings and its entrances. The system will be provided and operated in a way that is consistent with an individual's right to privacy.

The system will **NOT** be used to:

- Provide images to the World Wide Web.

- Record sound.
- Disclose to the media.

The CCTV surveillance system is owned by The Mulberry House School.

Overview of System.

- The CCTV system includes approximately 12 cameras.
- The CCTV system runs 24 hours a day, 7 days a week.
- The CCTV system is managed locally across the School site by Office staff and contractors acting on the School behalf.
- The CCTV system comprises fixed position cameras; monitors; digital recorders and public information signs.
- CCTV cameras are located at strategic points on site, principally at the entrance and exit point of sites and buildings, and in the gardens of the second school.
- CCTV signs will be prominently placed at strategic points and at entrance and exit points of the site to inform staff, students, visitors and members of the public that a CCTV installation is in use.
- Although every effort has been made to ensure maximum effectiveness of the CCTV system, it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

Data Protection Act 1998

- For the purpose of the Data Protection Act 1998, The Mulberry House School is the data controller.
- CCTV digital images that show a recognisable person are personal data and are covered by the Data Protection Act 1998. The provisions of this policy should be adhered to at all times.
- The Mulberry House School is required to register its processing of personal data (including CCTV) with the Information Commissioner's Office (ICO). The School's ICO notification registration number is Z2362454.
- Where new cameras are to be installed on School premises, Part 4 of the ICO's CCTV Code of Practice will be followed before installation:
- The appropriateness of and reasons for using CCTV will be assessed and documented.
- The purpose of the proposed CCTV system will be established and documented.
- Responsibility for day-to-day compliance with this policy will be established and documented.
- Consultation is required to ensure that the CCTV system is covered by the School's Notification with the Information Commissioner's Office ("ICO").

Access to Images

Access to images will be restricted to those staff who need to have access in accordance with the purposes of the system.

Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following:-

- Police and other law enforcement agencies where the images recorded could assist in a specific criminal enquiry and / or the prevention of terrorism and disorder.
- Prosecution agencies.
- Appropriate members of School staff (such as Human Resources) in the course of staff or student disciplinary proceedings (including prospective proceedings) to ensure compliance with the School's regulations and policies.

• People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries). Images that have been recorded may be viewed on site by the individual whose image has been captured and/or a uniformed police officer when responding to routine incidents which occurred on the same day. No copies may be taken off site.

Individual Access Rights

The Act gives individuals the right to access personal information about themselves, including CCTV images. All requests for access to a copy of CCTV footage by individuals should be made in writing to the school's Bursar, using the Subject Access Request form available at Annex A. The Headteaccher will liaise with relevant staff to determine whether the disclosure of the image will reveal third party information.

Requests for access to CCTV images must include:

• The date and time the images were recorded
• Information to identify the individual, if necessary
• The location of the CCTV camera
• Proof of Identity

The School will respond promptly and at the latest within 30 calendar days of receiving the request. If the School cannot comply with the request, the reasons will be documented. The requester will be advised of these in writing, where possible.

Access to Images by Third Parties

Unlike Data Subjects, third parties who wish to have a copy of CCTV images (i.e. images not of the person making the request) do not have a right of access to images under the DPA, and care must be taken when complying with such requests to ensure that neither the DPA, HRA or the CCTV Policy are breached. As noted above, requests from third parties will only be granted if the requestor falls within the following categories:

• Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry)
• Prosecution agencies
• Appropriate members of School staff (such as Human Resources and the Student Conduct and Appeals team) in the course of staff or student disciplinary proceedings (including prospective proceedings) to ensure compliance with the School's regulations and policies. All third party requests for access to a copy of CCTV footage by third parties should be made in writing to the school's Headteacher or Bursar. She will liaise with relevant staff to determine whether the disclosure of the image will reveal third party information.

Request to Prevent Processing

In addition to rights of access, Data Subjects also have rights under the DPA to prevent processing (i.e. monitoring and recording CCTV images) likely to cause substantial and unwarranted damage to that person, or prevent automated decision taking (i.e. through the use of visual recognition software) in relation to that person. Should any person visiting school have any concerns regarding the operation of the CCTV systems, the following procedure must be complied with:

• The Data Subject should be directed to the Headteacher or Bursar to determine whether the Data Subject is making a request to prevent processing or automated decision making. If the Headteacher or Bursar determines that the Data Subject is instead making a Subject Access Request, the procedure set out above will be followed.
• The Headteacher and/or Bursar will consider the request to prevent processing.

• The Headteacher and/or Bursar will provide a written response within twenty-one days of receiving the request to prevent processing or automated decision making, setting out their decision on the request. A copy of the request and response will be retained.

Retention and Disposal
Unless required for evidential purposes or the investigation of crime or otherwise required by law, recorded images will be retained for no longer than 31 days from the date of recording. At the end of their useful life all images on discs will be erased and securely disposed of as confidential waste. All still photographs and hard copy prints also will be securely disposed of as confidential waste.

Maintenance and Review
This Policy will be reviewed annually.
Complaints regarding the CCTV system and its operation must be made in writing to the Headteacher.

Enquiries
The School's Data Protection Policy is available from the School's Office and the website. General information about the Data Protection Act can be obtained from the Information Commissioner's Office;
(website www. ico.org.uk).

Individual members of staff can be personally liable in law under the terms of the 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, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as a disciplinary matter, and serious breaches could lead to dismissal.

ACCESS TO PERSONAL DATA REQUEST FROM THE MULBERRY HOUSE SCHOOL

DATA PROTECTION ACT 1998 Section 7.

Enquirer's Surname
……

Enquirer's
Forenames……..

Enquirer's Address
……

……
……..

……Postcode……
…….

Telephone Number
……..

Are you the person who is the subject of the records you are enquiring about
YES / NO (i.e. the "Data Subject")?

If NO,

Are you a parent as defined by the Education Act 1996 of a child who is the "Data Subject" of the YES / NO records you are enquiring about?

If YES, please state the name of child or children about whose personal data records you are enquiring

1. ……
   ……..
2. ……
   ……
3. ……
   ……..
4. ……
   ……

Description of Concern / Area of Concern

Description of Information or Topic(s) Requested (In your own words)

Additional information (please enclose a separate sheet if necessary)

Please despatch Reply to: *(if different from enquirer's details as stated on this form)*

Name

Address

Postcode

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent)

……
……..

Name of "Data Subject" (or Subject's Parent)

(PRINTED)
…….

Date
……

This form should be returned to
Jay Harley, Bursar and Data Manager
The Mulberry House School
7 Minster Road
London

NW2 3XL

DATA BREACH RECORD
FOR
THE MULBERRY HOUSE SCHOOL

Date	Person responsible for the breach				
Outline of Breach					
Which Data Subjects are involved?					
Data types involved					
Reported by					
Phone/email sent to Bursar	Y/N	Is this high risk	Y/N	Report to ICO	Y/N
Date reported to data subjects					
Preventative action suggestions – including training					
Notes					
Actions approved by				Date	