MICHAEL FARADAY SCHOOL

DATA PROTECTION POLICY

Contents

1. Aims

Michael Faraday Primary School uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

The school has a legal responsibility to comply with data protection legislation and other statutory provisions relating to the way in which it holds and processes personal data. The school, as a corporate body, is named as the data controller under the Data Protection Act 2018 (DPA 2018).

ICO Notification and Registration The school is required to 'notify' the Information Commissioner of the processing of personal data. This information is included in a public register which is available on the Information Commissioner's website. As a Data controller the school will register annually with the ICO as required in line with legislation.

Privacy Notices Every member of staff, member of the governing board, contractors, and partners of the school that hold its' personal information has to comply with the law when managing that information. Schools also have a duty to issue a privacy notice to all pupils/parents and its employees; these provide details of information collection and held, why it is held and the other parties to whom it may be passed on.

Data Controller As data controller personal data collected about staff, pupils, parents, governors, visitors and other individuals that is collected and held must be processed in accordance with the General Data Protection Regulation (GDPR) and the DPA 2018.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the GDPR. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically. The type of information that we may be required to handle include details of job applicants, current, past and prospective employees, pupils, parents / carers and other members of pupils' families, governors, suppliers and other individuals that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the GDPR and other legislation. The GDPR imposes restrictions on how we may use that information.

This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy by members of staff will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. Breach of the GDPR may expose the School to enforcement action by the Information Commissioner's Office (ICO), including the risk of fines. Furthermore,

certain breaches of the Act can give rise to personal criminal liability for the School's employees. At the very least, a breach of the GDPR could damage our reputation and have serious consequences for the School and for our stakeholders.

2. Scope of the Policy

We recognise that the correct and lawful treatment of personal data will maintain confidence in the school. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. **Under the GDPR, personal data' means any information relating to an identified or identifiable natural person ('data subject')**; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The school collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the school. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

3. Equal opportunities and inclusion

It is the right of all children, staff and visitors to the school, regardless of their gender, ethnicity, religion or beliefs, physical disability, ability, linguistic, cultural or home background, to have their personal information collected, stored and processed in line with the requirements of the current legislation.

4. Definitions of data protection terms

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.

Data controllers: are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our organisation for our own operational purposes.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data processors: include any person or organisation that is not a data user who processes personal data on our behalf and on our instructions. Employees of data

controllers are excluded from this definition but it could include suppliers which handle personal data on our school's behalf.

Data Protection Officer (DPO): is responsible for monitoring our compliance with data protection law.

Data subject: means a living, identified or identifiable individual about whom we hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data users: are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Personal data: means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach: any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

Processing: is any activity which is performed on personal data such as collection, recording, organisation, structuring, adaptation or alteration, using, storage, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special category personal data: includes information about a person's racial or ethnic origin, political opinions; religious or philosophical beliefs; trade union membership; physical or mental health or condition; genetic/biometric data held for purposes of identification or data about sexual orientation or an individual's sex life.

5. Roles and Responsibilities

This policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present pupils, employees, workers, or supplier contacts, website users or any other data subject.

Staff, those working on our behalf and volunteers

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf.

You must read, understand and comply when processing personal data on our behalf and attend training on its requirements. This policy sets out what we expect from you in order for the school to comply with applicable law. Your compliance with this policy is mandatory. You must also comply with all related policies and

guidelines given. Staff who do not comply with this policy may face disciplinary action.

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Ensuring that personal data held is accurate and up to date
- Ensuring that personal data held is not misused, lost or unlawfully disclosed

Data Protection Team

The Data Protection Team is made up of a Data Protection Officer (DPO), the Headteacher and the School Office Manager. The team is responsible for overseeing the implementation of this policy, monitoring the school's compliance with data protection law, and developing related policies and guidelines where applicable.

The DPT will provide an annual report of their activities directly to the Governing Body and, where relevant, will report any advice and recommendations on school data protection issues.

The DPT is also the first point of contact for individuals whose data the school processes, and for the ICO.

The Data Protection Team can be contacted at:
info@michaelfaraday.southwark.sch.uk
The DPO is David Powell who can be contacted at: dpo@sapphireskies.co.uk

The requirement that the DPO reports directly to the governing body ensures that the School's directors are made aware of the pertinent data protection issues. In the event that the School decides to take a certain course of action despite the DPO's advice to the contrary, the DPO should be given the opportunity to make their dissenting opinion clear to the Governing Body and to any other decision makers.

All staff must contact the Data Protection Team in the following circumstances:

- Where they are unsure or have questions about the operation of this policy; the purposes for which data may be used; retaining personal data; disclosing personal data or keeping personal data secure
- If there has been a data breach or a suspected data breach
- Where they are unsure if they have a lawful basis for processing personal data or wish to process for a different purpose than the one that the data was obtained
- Where they propose to engage in any activity that affects the rights of privacy of any individual i.e. where there is a legal obligation to carry out a DPIA
- Where they are unsure about what security or other measures they need to implement to protect personal data
- If they are engaging in an activity that may affect the privacy rights of individuals

- If they need any assistance dealing with any rights invoked by a data subject
- Where they are considering sharing personal data with third parties
- Where they are entering into contracts involving the processing of personal data by another organisation
- If they need to rely transfer personal data outside the European Economic Area

Where staff have concerns that this policy is not being followed by others they should report this immediately to the DPO. Where they wish to raise this formally they may do so under the school's whistleblowing policy for staff.

Governing Board
The governing board has overall responsibility for ensuring compliance with all relevant data protection obligations. All policies and documents related to data protection are reviewed annually by the Full Governing Body.

Headteacher
The headteacher has overall operational responsibility on a day-to-day basis for the implementation of the school's policies and procedures.

Data Protection Officer
The DPO is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues. The DPO is also a point of contact for individuals whose data the school processes who wish to raise any complaint regarding the school's processing where they remain dissatisfied with the school's response, and for the Information Commissioner's Office (ICO).

6. Personal Data Protection Principles

Michael Faraday Primary School adheres to the principles relating to processing of personal data set out in the GDPR which require personal data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation).
(d) Accurate and where necessary kept up to date (Accuracy).
(e) Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
(h) Made available to data subjects and data subjects allowed to exercise certain rights in relation to their personal data (Data Subject's Rights and Requests).

Michael Faraday Primary School is responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

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

- Inform data subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a privacy notice

- Check the quality and accuracy of the information held

- Apply the records management policies and procedures to ensure that information is not held longer than is necessary

- Ensure that when information is authorised for disposal it is done appropriately

- Ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system

- Only share personal information with others when it is necessary and legally appropriate to do so

- Set out clear procedures for responding to requests for access to personal information known as subject access request

- Train all staff so that they are aware of their responsibilities and of the school's relevant policies and procedures

7. Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. The school may only collect, process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the data subject.

The GDPR allows processing for specific purposes, some of which are set out below:

(a) the data subject has given his or her consent;
(b) the processing is necessary for the performance of a contract with the data subject;
(c) to meet our legal compliance obligations.;
(d) to protect the data subject's vital interests;
(e) the data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions - this is known as the public task

(f) to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and DPA 2018.

If our school offers online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

The purposes for which we process Personal Data to perform our public task are set out in the privacy notice issued by the school.

When we collect personal data directly from data subjects, including for human resources or employment purposes, we provide the data subject with all the information required by the GDPR including the identity of the Data Controller and DPO, how and why we will use, process, disclose, protect and retain that personal data through privacy notice.

The School has developed privacy notices for Pupils, Parents, Staff and Governors, The School wishes to adopt a layered approach to keeping people informed about how we process their Personal Data. This means that the privacy notice is just one of the tools we will use to communicate this information. School employees are expected to use other appropriate and proportionate methods to tell individuals how their Personal Data is being processed if Personal Data is being processed in a way that is not envisaged by our privacy notices and / or at the point when individuals are asked to provide their Personal Data, for example, where Personal Data is collected about visitors to Academy premises or if we ask people to complete forms requiring them to provide their Personal Data.

Consent

The School must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent. Consent is not the only lawful basis and there are likely to be many circumstances when we process Personal Data and our justification for doing so is based on a lawful basis other than Consent.
A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.
In the event that we are relying on Consent as a basis for Processing Personal Data about pupils, if a pupil is aged under 13, we will need to obtain Consent from the Parent(s). In the event that we require Consent for Processing Personal Data about pupils aged 13 or over, we will require the Consent is likely to be required if, for example, the school wishes to use a photo of a pupil on its website or on social media. **Consent is also required is also required before any pupils are signed up to online learning platforms. Such Consent must be from the Parent is the pupil is aged under 13.**

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.
Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data. Often we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Evidence and records of Consent must be maintained so that the School can demonstrate compliance with Consent requirements.

8. Sharing personal data

The school will not normally share personal data with anyone else without express consent, but may do so where:

- It is necessary for the performance of our public task
- There is an issue with a pupil or parent/carer that puts the safety of another individual at risk
- For safeguarding purposes
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we:
    - (i) Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - (ii) Establish either in the contract or as a standalone agreement, a data processing agreement to ensure the fair and lawful processing of any personal data we share
    - (iii) Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

The school will also share personal data with law enforcement and government bodies where we are legally required to do so, including for the following purposes:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff and for safeguarding purposes.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

The school may enter into information-specific sharing agreements with other public bodies for the purposes outlined above.

Criminal convictions and offences

There are separate safeguards in the GDPR for Personal Data relating to criminal convictions and offences.

It is likely that the School will Process Data about criminal convictions or offences. This may be as a result of pre-vetting checks we are required to undertake on staff and governors or due to information which we may acquire during the course of their employment or appointment.

In addition, from time to time we may acquire information about criminal convictions or offences involving pupils or Parents. This information is not routinely collected and is only likely to be processed by the School in specific circumstances, for example, if a child protection issue arises or if a parent / carer is involved in a criminal matter.

Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the data secure.

9. Subject access requests and other rights of individuals

Our data subjects have rights when it comes to how we handle their personal data. These include rights to:

- withdraw consent to processing at any time;
- receive certain information about how we process their data;
- request access to their personal data that we hold;
- prevent use of their personal data for direct marketing purposes;
- ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- restrict processing in specific circumstances;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which personal data is transferred outside of the EEA;
- object to decisions based solely on automated processing, including profiling (known as automated decision making ('ADM'));
- prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- be notified of a personal data breach which is likely to result in high risk to their rights and freedoms; and
- make a complaint to the Information Commissioner.

How to make a subject access request

The GDPR does not specify how to make a valid request.

You can make a subject access request verbally or in writing to any part of the school and not a specific contact point. We suggest however that you email the school if possible: info@michaelfaraday.southwark.sch.uk

We have one month to respond to your request.

GDPR requests for personal data are free in most cases unless the request is manifestly unfounded or excessive, when a "reasonable fee" for the administrative costs of complying with the request may be charged.

A reasonable fee will be charged based on administrative costs if an individual requests further copies of their data following a request.

When responding to requests, the school may ask the individual to provide 2 forms of identification and contact the individual to confirm that they made a request.

We may inform the requester that the school will comply within 3 months of receipt of the request, where a request is complex or numerous requests have been made, informing the requester of this within 1 month, and explaining why the extension is necessary.

The school will not disclose information if by doing so it:

- might cause serious harm to the physical or mental health of the pupil or another individual
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- is contained in adoption or parental order records
- is given to a court in proceedings concerning the child.

When the school refuses a request, the individual will be advised of the reason and that they have the right to complain to the ICO.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at the school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Parents, or those with parental responsibility, have a legal right to access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

Requests from pupils who are considered mature enough to understand their rights under the GDPR will be processed as a subject access request as outlined below and the data will be given directly to the pupil (subject to any exemptions that apply under the GDPR or other legislation). [As the age when a young person is deemed to be able to give Consent for online services is 13, we will use this age as a guide for when pupils may be considered mature enough to exercise their own subject access rights]. In every case it will be for the School as Data Controller, to assess whether the child is capable of understanding their rights under the GDPR and the implications of their actions, and so decide whether the Parent needs to

make the request on the child's behalf. A Parent would normally be expected to make a request on a child's behalf if the child is younger than 13 years of age. 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) where the pupil is aged under 13 (subject to any exemptions that apply under the Act or other legislation). If the Parent makes a request for their child's Personal Data and the child is aged 13 or older and / or the School considers the child to be mature enough to understand their rights under the GDPR, the School shall ask the pupil for their Consent to disclosure of the Personal Data if there is no other lawful basis for sharing the Personal Data with the Parent (subject to any enactment or guidance which permits the School to disclose the Personal Data to a Parent without the child's Consent). If Consent is not given to disclosure, the School shall not disclose the Personal Data if to do so would breach any of the data protection principles.
Where requests are "manifestly unfounded or excessive", in particular because they are repetitive, the School can:
charge a reasonable fee taking into account the administrative costs of providing the information; or refuse to respond.
Where we refuse to respond to a request, the response must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.
Members of staff should refer to any guidance issued by the ICO on Subject Access Requests and consult the DPO before refusing a request.
In the context of a school a subject access request is normally part of a broader complaint or concern from a Parent or may be connected to a disciplinary or grievance for an employee. Members of staff should therefore ensure that the broader context is taken into account when responding to a request and seek advice if required on managing the broader issue and the response to the request.

10. CCTV

Michael Faraday Primary School uses CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

The CCTV system that we use stores data for 5 days

Any enquiries about the CCTV system should be directed to the headteacher.

11. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

The school will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional

materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Marketing and promotional materials uses may include:

- Within school on notice boards and in school magazines, brochures, prospectuses newsletters, etc.
- Children's books to evidence their learning
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

When using photographs and videos in this way the school will not include any other personal information about the child, to ensure they cannot be identified, unless parent/carer consent is provided and safeguarding is not compromised.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

12. Protection of Biometric information

Legal Framework - Protection of Freedoms Act 2012 – Data Protection Act 2018 – GDPR - DfE guidance Protection of biometric information of children in schools and colleges

At Michael Faraday Primary School the written consent of at least one parent must be obtained before the biometric data is taken from the child and used. This applies to all pupils in schools and colleges under the age of 18.

In no circumstances can a child's biometric data be processed without written consent.

We will not process the biometric data of a pupil (under 18 years of age) where:

a) the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

b) no parent has consented in writing to the processing; or

c) a parent has objected in writing to such processing, even if another parent has given written consent.

We will where possible provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

We refer to the latest guidance published by the DfE for the implementation of policy https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

13. Record keeping

GDPR requires us to keep full and accurate records of all our data processing activities.

We keep and maintain accurate records reflecting our processing. These records include clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

14. Accountability, data protection by design

The school put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Passwords that are at least 8 characters long where possible containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our [online safety policy/ICT policy/acceptable use agreement/policy on acceptable use])

- Where the school needs to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and is adequately protected
- Confidential paper records will be kept in a locked filing cabinet, locked cupboard, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off site.
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted: teaching staff are provided with encrypted memory stick by the school.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff will not use their personal laptops or computers for school purposes if it involves the identifiable data of pupils, staff member or any other stake holder.
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- When sending confidential information by fax, staff will always check that the recipient is correct before sending.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
- Before sharing data, all staff members will ensure:

They are allowed to share it.
That adequate security is in place to protect it.
Who will receive the data has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

The physical security of the school's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Michael Faraday Primary School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The school Headteacher and Office Manager is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Storage of records
Michael Faraday Primary School has a responsibility to maintain its records and record keeping systems. When doing this, will take account of the following factors: -

- The most efficient and effective way of storing records and information;
- The confidential nature of the records and information stored;
- The security of the record systems used;
- Privacy and disclosure; and
- Their accessibility.

16. Retention schedule

The retention schedule broadly follows the guidelines from the Annual Review of School Records and Safe Data Destruction **IMRS (Information and Management Records Society)** checklist **approved by the DfE**.
Approved Information (hard copy and electronic) will be retained for at least the period specified in the retention schedule. When managing records, the school will adhere to the standard retention times listed within that schedule. Paper and Electronic records will be regularly monitored by school staff. The retention periods are based on business needs and legal requirements.

17. Destruction of records

Where records have been identified for destruction they should be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

We will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

19. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. A personal data breach is more than just losing personal data. It is a breach of security leading to the accidental or lawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

In the unlikely event of a suspected data breach, we will follow the school's Personal Data Breach Procedure (see **Appendix A**) and take all steps we can to remedy the breach that has occurred.

When appropriate, we will report the data breach to the ICO within 72 hours.

20. Training

All staff and governors are provided with data protection training as part of their induction process.

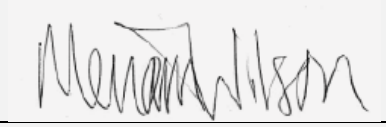
Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

21. Review and Monitoring arrangements

This policy is reviewed at least annually by the School Office Manager, the Data Protection Officer (DPO), the Governor with responsibility for GDPR and the Headteacher.

For help or advice on this policy and further specialist information may be sought form the school's DPO please contact the Data Protection Team at: info@michaelfaraday.southwark.sch.uk

This policy is reviewed and ratified by the Full Governing Body.

Agreed by the Governing Body on	November 2020
Signed (Chair)	
Review Date	Spring 2023

***Appendix A*: Personal data breach procedure**

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

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

- The DPT will decide if there are any conflicts of interest within the team and, if there are,

the relevant person will step away from the process.

- The DPT will investigate the report, and determine whether a breach has occurred. To

decide, the DPT will consider whether personal data has been accidentally or unlawfully:

- lost
- stolen
- destroyed
- altered
- disclosed or made available where it should not have been
- made available to unauthorised people.

- The DPT will alert the Chair of Governors
- The DPT will make all reasonable efforts to contain and minimise the impact of the

breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

- The DPT will assess the potential consequences, based on how serious they are, and

how likely they are to happen

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

- loss of control over their data
- discrimination
- identify theft or fraud
- financial loss
- unauthorised reversal of pseudonymisation (for example, key-coding)
- damage to reputation
- loss of confidentiality
- any other significant economic or social disadvantage to the individual(s) concerned.

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

- The DPT will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- a description of the nature of the personal data breach including, where possible:

- the categories and approximate number of individuals concerned
- the categories and approximate number of personal data records concerned

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

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

information as soon as possible.

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

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

- The DPT will notify any relevant third parties who can help mitigate the loss to individuals

– for example, the police, insurers, banks or credit card companies

- The DPT will document each breach, irrespective of whether it is reported to the ICO.

For each breach, this record will include the:
- facts and cause
- effects
- action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's computer system. The DPT will meet

to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

In the event of a data breach, the school will take action to mitigate the impact of the

breach, particularly if it involves sensitive information. The school will review the effectiveness of these actions and amend them as necessary after any data breach.