# Data Protection Policy

# Emmanuel Community School

# Data Protection Policy

**Contents** **Page**



## 1. Introduction

Emmanuel Community 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 Act.

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 at: https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

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.

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 (UK GDPR) and the Data Protection Act 2018 (DPA 2018) as is currently set out in the Data Protection Bill.

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 General Data Protection Regulation. 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.

## 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 UK 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. 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 business for our own commercial 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 Schools 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.

## 4. 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 and those working on our behalf**
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

**All staff must contact the DPO 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
- 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 Privacy Impact Assessment
- Where they are unsure about what security or other measures they need to implement to protect Personal Data
- 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

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 Schools' Policy and Procedure for reporting of Data Protection Infringements by Employees (Appendix 1).

**Governing Board**
The governing board or Governing Body has overall responsibility for ensuring compliance with all relevant data protection obligations.

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

**UK Data Protection Officer**
The data protection officer (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 ICO.

## 5. Personal Data Protection Principles

We adhere 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).

We are 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 schools relevant policies and procedures

## 6. Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK 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 Data Protection Act 2018.

If we offer 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 a Fair Processing (Privacy) Notice.

## 7. 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
- 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

We 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.

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.

We may enter into Information Specific Sharing Agreements with other public bodies for the purposes outlined above.

## 8. 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:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about how we process their data;

(c) request access to their Personal Data that we hold;

(d) prevent use of their Personal Data for direct marketing purposes;

(e) 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;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling (known as Automated Decision Making ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the Information Commissioner; and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

Where an individual exercises their rights of subject access this will be dealt with under the schools Subject Access Request Policy and Procedure.

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.

## 9. Photographs and videos

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

We 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.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

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.

See our [child protection and safeguarding policy/photography policy/other relevant policy] for more information on our use of photographs and videos.

## 10. Record keeping

The UK 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.

## 11. Accountability, Data protection by design

We 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 privacy 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

## 12. 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:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long 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 we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

## 13. Disposal of records

Personal data that is no longer needed will be disposed of securely as defined in our School Retention Schedule.. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, 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.

## 14. 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 Schools Personal Data Breach Procedure 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.

## 15. 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.

## 16. Review and Monitoring arrangements

This policy will be reviewed and updated as and when necessary e.g. when the Data Protection Bill becomes law the Data Protection Act 2018. The DPO will review this policy at every annual audit and report any necessary changes to the governing board.

Further specialist information and advice may be sought from the Schools Data Protection Officer (see details below)

For help or advice on this policy please contact:

**Maryline Alvis**
Education Data Protection Officer via
Education Data Protection Service Team
Governance & Law
London Borough of Waltham Forest
Email: edposervice@walthamforest.gov.uk

Or

Mrs. T. Oluwatudimu
Data Protection Officer for Emmanuel Community School

Approved by:
Mrs Oluwatudimu Date: Nov 2018

Last reviewed on: Date: Nov 2021

Next review due by: Date: Nov 2023

# Appendix 1

**Policy and Procedure for reporting of Data Protection infringements by Employees**

**Emmanuel Community School Policy and Procedure for reporting of Data Protection infringements by Employees**

## 1. INTRODUCTION

1.1 Employees are often the first to realise that there may be something seriously wrong within the School. However, they may not express their concerns because they feel that speaking up would be disloyal to their colleagues or to the School. They may also fear harassment or victimisation. In these circumstances it may be easier to ignore the concern rather than report what may just be a suspicion of malpractice. The School has a Whistleblowing Policy for employees under which they may raise any such concerns where their disclosures relate to conduct which is an offence or a breach of law; disclosures related to miscarriages of justice; the unauthorised use of public funds; possible fraud and corruption and/or other unethical conduct. Under the General Data Protection Regulations data controllers are required to provide their staff with a procedure whereby they may safely raise concerns over whether as a data controller there is compliance with the data protection legislation.

1.2 This Policy and procedure is for employees of the School and should be used when a member of staff has concerns regarding compliance with data protection legislation that they feel they need to raise formally.

1.3 Emmanuel Community School is committed to the highest possible standards of compliance with the UK GDPR and data protection. In line with that commitment we expect employees, who have serious concerns about any aspect of the School's

compliance with data protection to come forward and voice those concerns. It is recognised that most cases will have to proceed on a confidential basis.

1.4 The policy document makes it clear that you can do so without fear of victimisation, subsequent discrimination or disadvantage. This policy is intended to encourage and enable employees to raise serious concerns within the School rather than overlooking a problem or 'blowing the whistle' outside.

1.5 The policy applies to all employees working for the School on School premises, for example, agency staff, consultants, etc. It also covers suppliers and those providing services under a contract with the School.

1.6 These procedures are in addition to the School's complaints procedures, Whistleblowing procedure and other statutory reporting procedures.

## 2. AIMS AND SCOPE OF THIS POLICY

2.1 This policy aims to:

- encourage you to feel confident in raising serious concerns and to question and act upon concerns about the school's data protection practices
- provide avenues for you to raise those concerns and receive feedback on any action taken
- ensure that you receive a response to your concerns and that you are aware of how to pursue them if you are not satisfied
- Reassure you that you will be protected from possible reprisals or victimisation if you have a reasonable belief that you have raised those concerns in good faith.

2.2 There are existing procedures in place to enable you to lodge a grievance relating to your own employment, seek access to your own information, or complain regarding the way in which the school is handling your personal data. This policy is intended to cover major concerns that fall outside the scope of other procedures. These include but are not limited to:

- Concerns over practices observed by you that adversely impacts on the security of personal data held by the school
- Concerns over unauthorised disclosure or use of personal data held by the school
- Concerns over actions leading to the corruption or loss of integrity of any of the personal data held by the school
- other unethical conduct which you believe is a breach of the schools obligations as a Data Controller

2.3 Thus, any serious concerns that you have about any aspect of the Schools handling of personal data or of others acting on behalf of the School in their handling of personal data can be reported under this policy.

2.4 This policy does not replace the Schools complaints procedure.

## 3. SAFEGUARDS

3.1 Harassment or Victimisation

3.1.1 The School is committed to good practice and high standards and wants to be supportive of employees.

3.1.2 The School recognises that the decision to report a concern can be a difficult one to make. If what you are saying is true, you will have nothing to fear because you will be doing your duty to your employer and those for whom you are providing a service.

3.1.3 The School will not tolerate any harassment or victimisation (including informal pressures) from your colleagues, peers, managers or from external sources, and will take appropriate action to protect you when you raise a concern in good faith.

3.1.4 Any investigation into allegations of potential malpractice will not influence or be influenced by any disciplinary or redundancy procedures that already affect you.

### 3.2 Confidentiality

3.2.1. All concerns will be treated in confidence and the School will keep your identity confidential if you so wish. At the appropriate time, however, you may need to come forward as a witness.

## 4. ANONYMOUS ALLEGATIONS

4.1 This policy encourages you to put your name to your allegation whenever possible.

4.2 Concerns expressed anonymously are much less powerful but will be considered at the discretion of the School.

4.3 In exercising this discretion the factors to be taken into account would include:

- the seriousness of the issues raised
- the credibility of the concern; and
- the likelihood of confirming the allegation from attributable sources.

## 5. UNTRUE ALLEGATIONS

5.1. If you make an allegation in good faith, but it is not confirmed by the investigation, no action will be taken against you. If, however, you make an allegation frivolously, maliciously or for personal gain, disciplinary action may be taken against you.

## 6. HOW TO RAISE A CONCERN

6.1 As a first step, you will normally raise concerns with your immediate manager or their superior. This depends, however, on the seriousness and sensitivity of the issues involved

and who is suspected of the malpractice. For example, if you believe that management is involved you will approach the:-

Chair of Governors

6.2 Concerns may be raised verbally or in writing. Staff who wish to make a written report are invited to include the following information:

- the background and history of the concern (giving relevant dates);
- the reason why you are particularly concerned about the situation.

6.3 The earlier you express the concern the easier it is to take action.

6.4 Although you are not expected to prove beyond doubt the truth of an allegation, you will need to demonstrate to the person contacted that there are reasonable grounds for your concern.

6.5 If ultimately you feel you have to take the matter externally to the Information Commissioner their details are listed at Section 9 of this policy.

6.6 You may wish to consider discussing your concern with a colleague first and you may find it easier to raise the matter if there are two (or more) of you who have had the same experience or concerns.

6.7 You may invite your trade union, professional association representative or a friend to be present during any meetings or interviews in connection with the concerns you have raised.

## 7. HOW THE SCHOOL WILL RESPOND

7.1 The School will respond to your concerns. Do not forget that testing out your concerns is not the same as either accepting or rejecting them.

7.2 Where appropriate, the matters raised may:

- be investigated by the Data Protection Officer
- be referred to the Information Commissioner's Officer if found to be a reportable breach of data protection legislation
- lead to a disciplinary investigation
- form the subject of an independent inquiry.

7.3 In order to protect individuals and those accused of misdeeds or possible malpractice, initial enquiries will be made to decide whether is appropriate and, if so, what form it will take. The overriding principle which the School will have in mind is the necessity to provide assurance that the school complies with its' data protection obligations.

7.4 Some concerns may be resolved by agreed action without the need for investigation. If urgent action is required this will be taken before any investigation is conducted.

7.5 Within ten working days of a concern being raised, the responsible person will write to you:

- acknowledging that the concern has been received
- indicating how we propose to deal with the matter
- giving an estimate of how long it will take to provide a final response
- telling you whether any initial enquiries have been made
- supplying you with information on staff support mechanisms, and
- telling you whether further investigations will take place and if not, why not.

7.6 The amount of contact between the officers considering the issues and you will depend on the nature of the matters raised, the potential difficulties involved and the clarity of the information provided. If necessary, the School will seek further information from you.

7.7 Where any meeting is arranged, off-site if you so wish, you can be accompanied by a union or professional association representative or a friend.

7.8 The School will take steps to minimise any difficulties which you may experience as a result of raising a concern. For instance, if you are required to give evidence in criminal or disciplinary proceedings the School will arrange for you to receive advice about the procedure.

7.9 The School accepts that you need to be assured that the matter has been properly addressed. Thus, subject to legal constraints, we will inform you of the outcome of any investigation.

## 8. THE RESPONSIBLE OFFICER

8.1 The Chair of Governors has overall responsibility for the Policy. The day to day maintenance and operation of the policy will be undertaken by the Head Teacher. They will maintain a record of concerns raised and the outcome (but in a form which does not endanger your confidentiality) and will report as necessary to the Governors/Board of the School.

## 9. HOW THE MATTER CAN BE TAKEN FURTHER

9.1 This policy is intended to provide you with an avenue within the School to raise concerns. The School hopes you will be satisfied with any action taken. If you are not, and if you feel it is right to take the matter outside the School, to the Information Commissioner their contact details are:

Information Commissioner

Information Commissioner's Office, Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF

Tel: 0303 123 1113

Email: casework@ico.org.uk.

Or go to their website at: https://ico.org.uk/global/contact-us/email/

9.2 If you do take the matter outside the School, you must ensure that you do not disclose confidential information in a manner that is in breach of the Schools Data Protection Policy, e.g. you must not disclose personal data and so any reporting by you should, whilst explaining your concerns, should not disclose the identity of any individuals, be they students, parents, or members of staff. Should the ICO in response to any referral by you seek information from the School the School will co-operate fully and will provide such information to the ICO as is necessary for the purposes of any follow-up investigation by them.

# Appendix 2
# Personal Data Breach Procedure

## Personal Data Breach Procedure
## Information Security Incident Reporting Policy and Procedures

**Contents**

## 1. INTRODUCTION

Emmanuel Community School processes personal data including special category personal data daily and it is essential that procedures are in place to ensure any threat to the security of that information is minimised and any breaches of the duties in respect of that information are identified and remedied. Any incident that compromises the security of that information, or the ICT system on which it resides, must be managed appropriately and in accordance with legislation and guidance provided by the Information Commissioners Office (ICO).

## 2. PURPOSE

The purpose of this policy is to ensure that the School reacts appropriately to mitigate the risks associated with actual or suspected security incidents relating to information systems and data. The School recognises that there are risks associated with users accessing and handling information to conduct official School business.

This policy aims to mitigate the following risks:

- Reduce the impact of information security incidents by ensuring they are followed up correctly
- Improve compliance by ensuring serious security incidents are reported to the appropriate external organisations
- To help identify areas for improvement to decrease the risk and impact of future incidents.

## 3. SCOPE

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

All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of the School's systems and the information that they use or manipulate.

All users have a role to play and a contribution to make to the safe and secure use of information and communications technology, and the information that it processes or stores.

You must read, understand and comply with this Policy. 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.

## 4. OBJECTIVES

The main objective of this policy is to ensure security incidents relating to School information and ICT systems are reported, recorded and investigated in accordance with the School's and legislative standards.

## 5. LEGAL REQUIREMENTS

As data controller personal data collected about staff, pupils, parents, governors, visitors and other individuals that is collected and held must be protected from unlawful misuse, loss, theft, accidental disclosure, destruction, corruption or alternation in accordance with the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) as is currently set out in the Data Protection Bill.

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

## 6. COMPLIANCE

If any user is found to have breached this policy, they may be subject to the School's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).
Non-compliance with this policy could have a significant effect on the efficient operation of the School and may result in significant financial loss.
The General Data Protection Regulation (UK GDPR) introduces a duty for us to report personal data breaches which are significant to the Information Commissioner. This must be done within 72 hours of the breach, where feasible.
If the breach is expected to adversely impact (or has a high likelihood of impacting) individual's rights and freedoms, we must also inform those individuals 'without undue delay'.
We will keep a record of any personal data breaches, regardless of whether we are required to notify.

## 7. DEFINITION

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.
This policy needs to be applied as soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident.
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.
Examples of the most common personal data breaches and information security incidents are listed below. It should be noted that this list is not exhaustive.

- Giving information to someone who should not have access to it – this could be verbally, in writing or electronically.
- Theft / loss of a confidential paper
- Sending personal data to an incorrect recipient .e.g. groups of recipients such as 'all staff' by mistake.
- Sending a text message containing personal data to all parents by mistake.
- Writing down your password and leaving it on display or somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.
- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- Computer infected by a Virus or other malware.
- Finding data that has been changed by an unauthorised person.
- Use of unapproved or unlicensed software on School ICT equipment.
- Accessing a computer database using someone else's authorisation (e.g. someone else's user ID and password).

- Changes to information or data or system hardware, firmware, or software characteristics without the School's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person

## 8. PROCEDURE FOR PERSONAL DATA BREACH AND SECURITY INCIDENT HANDLING

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact Mrs. Oluwatudimu who is the person designated as the key point of contact for Personal Data Breaches. You should preserve all evidence relating to the potential Personal Data Breach.
On finding or causing a breach, or potential breach, Mrs. Oluwatudimu must immediately notify the Data Protection Officer and take immediate remedial steps to mitigate and remedy the breach that has occurred. All reasonable steps must be taken to retrieve any information that has been unlawfully disclosed.
The EDPO **Maryline Alvis** will provide advice on the immediate steps to be taken, investigate the report, and determine whether a breach has occurred.
The EDPO will alert the Head teacher and the chair of governors if not already notified.
The EDPO will assist Mrs. Oluwatudimu and relevant staff members or data processors where necessary to mitigate risk and impact.
The actions to be taken will be relevant to specific data types. The actions to minimise the impact of data breaches are set out below. These must, where relevant, be taken to mitigate the impact of different types of data breach. Breaches involving particularly risky or sensitive information must be acted upon swiftly and steps followed through.
We will review the effectiveness of these actions and amend them as necessary after any data breach.

**EXAMPLE:**
If sensitive information has been disclosed via email (including safeguarding records) or other special category data (sensitive information) such as health information is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error. Where this is unsuccessful or not possible immediate steps should be taken to contact the recipient with instructions to them to delete the email.
If the sender is unavailable or cannot recall the email for any reason, the nominated contact (Mrs. Oluwatudimu) will ask the ICT department to recall it.
Where members of staff receive personal data sent in error they must alert the sender and Mrs. Oluwatudimu as soon as they become aware of the error.
In any cases where the recall is unsuccessful, Mrs. Oluwatudimu will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way. Mrs. Oluwatudimu will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
The EDPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

**INVESTIGATION AND REPORT**
The EDPO will carry out an internet search to check that the information has not been made public, if it has; we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

The EDPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
The EDPO 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 EDPO 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 EDPO must notify the ICO WITHIN 72 hours of the personal data breach coming to the attention of Mrs. Oluwatudimu.
The EDPO 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.
Where the ICO must be notified, the EDPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the EDPO 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 EDPO
- 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 EDPO 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 EDPO expects to have further information. The EDPO will submit the remaining information as soon as possible.
The EDPO 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 EDPO 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 EDPO
- 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

**REPORT**
The EDPO 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 in a spreadsheet on the shared office drive.

**REVIEW AND PLANNING**
The EDPO and Headteacher will meet to review what happened and how it can be prevented from happening again. This meeting will happen as soon as reasonably possible. A report of data protection breaches and information security incidents will be presented to the Governing Board.

## 9. REPORTING INFORMATION SECURITY WEAKNESSES FOR ALL EMPLOYEES

Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such action may be considered to be misuse of information assets.
Weaknesses reported to third party application and service providers by employees must also be reported internally to the Schools ICT. The provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded and reported.
Security events can include:

- Uncontrolled system changes
- Access violations – e.g. password sharing
- Breaches of physical security
- Non-compliance with policies
- Repeated lock out of user accounts
- Flooding of the system with emails
- Malicious software (virus infections)
- Unscheduled shutdowns, system errors or overloads

Security weaknesses can include:

- Inadequate firewall or antivirus protection
- System malfunctions or overloads
- Malfunctions of software applications
- Human error

All events must be logged with ICT and reported to Mrs. Oluwatudimu. A risk impact assessment must be carried out, and mitigation action including implementation timeframes identified.

## 10. REVIEW AND MONITORING ARRANGEMENTS

This policy will be reviewed and updated as and when necessary e.g. when the Data Protection Bill becomes law the Data Protection Act 2018. The DPO will review this policy at every annual audit and report any necessary changes to the governing board.
Further specialist information and advice may be sought from the Schools Data Protection Officer (see details below)
For help or advice on this policy please contact:

**Maryline Alvis**
Education Data Protection Officer via
Education Data Protection Service Team
Governance & Law
London Borough of Waltham Forest
Email: edposervice@walthamforest.gov.uk
Or
Mrs. Oluwatudimu
Data Protection Officer for Emmanuel Community School

Approved by:
Mrs Oluwatudimu Date: Nov 2018

Last reviewed on: Date: Nov 2021

Next review due by: Date: Nov 2023

# Appendix 3
## Subject Access Request Procedure

**Emmanuel Community School Subject Access Request Procedure**

**Access to information**

Current and former pupils can request access to the information/data held on them by making a **subject access request.** On occasions a parent or carer of a pupil may also make a subject access request that seeks access to personal data held that relates to either themselves and/or the pupil they are concerned with.

All subject access requests for data held by our school procedures should be sent to Mrs. T. Oluwatudimu. All requests will be dealt with within 30 calendar days.

NB: This procedure does not apply when a parent is exercising their rights under The Education (Pupil Information) (England) Regulations 2005 (SI 2005/1437) (Pupil Information Regulations) of pupils at maintained schools the right to access their children's educational records and set out when such requests may be refused.

**Actioning a Subject Access Request**

1. Requests for information must be made in writing, which includes email, and be addressed to the Headteacher. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be reasonably established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Examples of evidence of identity can be established by requesting production of:

- passport
- driving licence

- utility bills with the current address
- Birth / Marriage certificate
- P45 / P60
- Credit Card or Mortgage statement

*This list is not exhaustive*.

3. Any individual has the right of access to information held about them.

However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent, an individual with parental responsibility or guardian shall make the decision on behalf of the child. It is important to recognise that children are entitled to privacy and that there may be a duty of confidentiality owed to them which must be adhered to. Before discussing with a parent that a child has made a subject access request the school will ask the child whether they object to their parents becoming aware of this request and will abide by the child's wishes unless there is an overriding public interest reason why that should not be the case. Before proceeding with informing a parent in these circumstances advice of the Data Protection Officer should be sought.

4. The school does not charge for the provision of information, dependent upon the following:

- If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.
- A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.
- When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

5. The response time for Subject Access Requests, once officially received, is 30 calendar days. However the 30 calendar days will not commence until after receipt of fees or clarification of information sought. The school will respond **promptly** to a subject access request.

6. The General Data Protection Regulation (UK GDPR) allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure.

7. Third party information is that which has been provided by another person, this may be another pupil, parent, member of the family. The school must consider whether the information held was given in circumstances where an expectation of confidentiality has arisen. The school must also consider whether or not the information is already known to the pupil or parent concerned. If information is in the public domain, and/or the school is satisfied that the information is already known then it may be disclosed. Information provided by the Police, Local Authority, Health Care professional or another school may also have been provided to the school in the expectation that it will be held confidentially. Where the information is a health record made by a health care professional the consent of that professional must be sought before it may be released.

8. Any information which, it is believed may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. There is no right to access for information kept individually by teachers or other staff in notebooks or teacher mark books. These include such records generated and held electronically.

10. If there are concerns over the disclosure of information then additional advice should be sought from the schools' Data Protection Officer.

11. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

12. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

13. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.

**Complaints**

1. Complaints about the handling of a subject access request should be made directly to the Education data protection officer (EDPO) who is responsible for overseeing the implementation of this policy and monitoring our Schools compliance with data protection law.

The EDPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Our EDPO is Maryline Alvis and is contactable via edposervice@walthamforest.gov.uk.

2. Complaints about the above procedures should be made to the Chairperson of the Governing Body who will both monitor and decide whether it is appropriate for the complaint to be dealt with in accordance with the school's Complaints Policy. For information regarding subject access requests https://ico.org.uk/for-the-public/personal-information/

Complaints which are not appropriate to be dealt with through the school's Complaints Policy can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

**Appendix 4:**
**Records Retention Schedule**

**Appendix 5:**
**Privacy Notices**