Emerson Park Academy

DATA PROTECTION POLICY

Date Reviewed: January 2023

Next Review Date: January 2024

Contents

1. AIMS

The Academy aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 1998 and the General Data Protection Regulation 2018.

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

2. LEGAL FRAMEWORK

This policy meets the requirements of the Data Protection Act 2018 and is based on guidance published by the Information Commissioner's Office, ICO's code of practice for subject access requests and model privacy notices published by the Department for Education.

In addition, this policy complies with the General Data Protection Regulation, May 2018.

This policy has due regard to legislation, including, but not limited to the following:

- The Freedom of Information Act 2000
- Protection of Freedoms Act 2012 when referring to the use of biometric data.
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Academy Standards and Framework Act 1998
- The ICO's code of practice for the use of surveillance cameras and personal information.
- In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005 (As amended in 2016), which gives parents the right of access to their child's educational record.

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- Department for Education (August 2018) 'Data protection: a toolkit for Academys'

This policy will be implemented in conjunction with the Academy's Privacy Notice.

3. DEFINITIONS

Applicable Data

For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

Definitions Table

Term	Definition
Personal data	Relates to a living individual who can be identified from the data or other information held/likely to be held by the data controller (even where they are not named e.g. from a reference number), including opinions about the individual or what is intended for them. The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.
Sensitive personal data	Data such as: ● Contact details ● Racial or ethnic origin ● Political opinions ● Religious beliefs, or beliefs of a similar nature ● Where a person is a member of a trade union ● Physical and mental health ● Sexual orientation ● Whether a person has committed, or is alleged to have committed, an offence ● Criminal convictions The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Processing	Obtaining, recording, holding information, or carrying out operations on data including: • Organisation, adaptation or alteration of data • Retrieval, consultation or use of data • Disclosure of data by transmission, dissemination or other ways of making available • Alignment, combination, blocking, erasure or destruction of data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller
Inaccurate data	Incorrect or misleading data.
Recipient	Anyone to whom data are disclosed unless disclosure is being made as part of a legal inquiry.
Third party	Any person other than the data subject, the data controller, any data processor or other person authorised to process data .

4. DATA PROTECTION ACT 2018 PRINCIPLES

The **Data Protection Act 2018** is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 2018
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

Under the **Data Protection Act 2018,** the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

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

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

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

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

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

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

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

5. ROLES AND RESPONSIBILITIES

The Governing Board has overall responsibility for ensuring that the Academy complies with its obligations and all current legislations.

EPA is the data controller for the purposes of the act and therefore have overall responsibility for compliance with the DPA 2018. The Academy processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. EPA is registered as a data controller with the ICO and will renew the registration annually or as otherwise legally required.

EPA have delegated responsibility to the Headteacher to ensure compliance with this policy within the day-to-day activities of the Academy.

EPA has appointed a Designated Data Protection Officer (DPO). The DPO is responsible and required to perform several tasks under GDPR. They include the following:

- Inform and advise the organisation and its employees of their data protection obligations under the Data Protection Act 2018.
- Monitor the organisation's compliance with the Data Protection Act 2018 and internal data protection policies and procedures. This will include monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits.
- Advise on the necessity of data protection impact assessments (DPIAs), the manner of their implementation and outcomes.
- Serve as the contact point to the data protection authorities for all data protection issues, including data breach reporting.
- Serve as the contact point for individuals (data subjects) on privacy matters, including subject access requests.

Staff are responsible for

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Academy of any changes to their personal data, such as a change of address
- Contacting the designated DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. ACCOUNTABILITY

The Academy implements appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the Data Protection Act.

The Academy provides comprehensive, clear and transparent privacy notice.

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

The Academy implements measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Regularly management and improvement of our security features.

Data protection impact assessments will be used, where appropriate. For example, DPIAs have been completed for SIMs (the Academy's Management Information System) and CPOMS (the Academy's new Safeguarding platform).

7. PRIVACY / FAIR PROCESSING NOTICE

A privacy notice is a statement that describes how the Academy, uses, retains and discloses personal information. Different Organisations sometimes use different terms and it can be referred to as a privacy statement, a fair processing notice or a privacy policy.

To ensure that we process your personal data fairly and lawfully we are required to inform you:

- What Information we collect, hold and share.
- Why we collect and use this information
- The lawful basis on which we use this information.
- Who we share this information with.
- Why we share this information.
- Our Data collection requirements.
- How you can access this data and your rights.

This information also explains what rights you have to control how we use your information. The law determines how organisations can use personal information, relevant educational legislation, and the common law duty of confidentiality.

7.1 Privacy notice

Please refer to the *Privacy notice* on the Academy's website.

8. LAWFUL PROCESSING

The legal basis for processing data will be identified and documented prior to data being processed.

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Academy can fulfil a contract with the individual, or the individual has asked the Academy to take specific steps before entering into a contract
- The data needs to be processed so that the Academy can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the Academy, as a public authority, can perform a task in the public interest**,** and carry out its official functions
- The data needs to be processed for the legitimate interests of the Academy or a third party(provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
    - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.

- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

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 where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

8.1 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Academy's record of processing activities.

9. CONSENT

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

The Academy will ensure that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.

Consent can be withdrawn by the individual at any time.

The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child.

10. THE RIGHT TO BE INFORMED

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a child, the Academy will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative and the designated DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
  o Withdraw consent at any time.
  o Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

10.1 **Sharing personal data**
The Academy will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- The Academy needs to liaise with other agencies, will seek consent as necessary before doing this
- The Academy's suppliers or contractors need data to enable us to provide services to our staff and pupils
  – for example, IT companies. When doing this, The Academy will:
    - o Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- 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 Academy will also share personal data with law enforcement and government bodies where we are legallyrequired to do so, including for:

- 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

The Academy 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.

11. THE RIGHT OF ACCESS

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The Academy will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the Academy may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the Academy holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the Academy will ask the individual to specify the information the request is in relation to.

12. THE RIGHT TO RECTIFICATION

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the Academy will inform them of the rectification where possible.

Where appropriate, the Academy will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the Academy will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

13. THE RIGHT TO ERASURE

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The Academy has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information of the Academy
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the Academy will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

14. THE RIGHT TO RESTRICT PROCESSING

Individuals have the right to block or suppress the Academy's processing of personal data.

In the event that processing is restricted, the Academy will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The Academy will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Academy has verified the accuracy of the data
- Where an individual has objected to the processing and the Academy is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the Academy no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the Academy will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The Academy will inform individuals when a restriction on processing has been lifted.

15. THE RIGHT TO DATA PORTABILITY

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form. The Academy will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The Academy is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the Academy will consider whether providing the information would prejudice the rights of any other individual.

The Academy will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the time frame can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the Academy will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

16. The right to object

The Academy will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The Academy will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Academy can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The Academy will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Academy cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Academy is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the Academy will offer a method for individuals to object online.

17. PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS

The Academy will act in accordance with the Data Protection Act by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Academy has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Academy's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the Academy to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to OPHS's reputation which might otherwise occur.

A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

The Academy will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the Academy will consult the ICO / the Local Authority to seek its opinion as to whether the processing operation complies with the Data Protection Act.

18. DATA BREACHES

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The Principal will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training. The Academy will makeall reasonable endeavours to ensure that there are no personal data breaches.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

In the unlikely event of a suspected data breach, we will follow the procedure set out in **Appendix 2.** When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a Academy context may include, but are not limited to:

- A non-anonymised dataset being published on the Academy website which shows the examresults of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of an Academy laptop containing non-encrypted personal data about pupils

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Academy will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the Academy, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure itself to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

19. DATA SECURITY

Confidential paper records will be kept in a locked filing cabinet, 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.

All electronic devices are password-protected to protect the information on the device in case of theft.

Where possible, the Academy enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff and governors will not use their personal laptops or computers for Academy purposes. If staff use their phones, then they are responsible for ensuring that the data is fully protected.

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 Academy 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 Academy containing sensitive information are supervised at all times.

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

The Academy takes its duties under the Data Protection Act seriously and any unauthorised disclosure may result in disciplinary action.

The designated Data Protection Officer is responsible for continuity and recovery measures are in place to ensure the security of protected data.

20. PUBLICATION OF INFORMATION

The Academy publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

The Academy will not publish any personal information, including photos, on its website without the permission of the affected individual.

When uploading information to the Academy website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

21. CCTV AND PHOTOGRAPHY

The Academy understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The Academy notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

Emerson Park Academy has a statutory responsibility for the protection of its property, equipment and other plant as well a s providing a sense of security to its employees, students and invitees to its

premises. Emerson Park Academy owes a duty of care under the provisions of Safety, Health and Welfare at Work Act 2005 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of the Academy's community by integrating the best practices governing the public and private surveillance of its premises.

The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring employee performance.

Information obtained through the CCTV system may only be released when authorised by the Headteacher/Designated Data Protection Officer, following consultation with the Chair of Governors. Any requests for CCTV recordings/images from the police will be fully recorded. If a law enforcement authority, such as the police, is seeking a recording for a specific investigation, the police may require a warrant and accordingly any such request made by the police should be requested in writing and the Academy will immediately seek legal advice.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the Academy, including Equality & Diversity Policy, Dignity at Work Policy, Codes of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies, including the provisions set down in equality and other educational and related legislation.

This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc.

Video monitoring of public areas for security purposes within the Academy premises is limited to uses that do not violate the individual's reasonable expectation to privacy.

Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the Academy.

All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by Emerson Park Academy. Recognisable images captured by CCTV systems are "personal data." They are therefore subject to the provisions of this Data Protection Act.

CCTV systems are installed (both internally and externally) in premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environmentss of the premises during both the daylight and night hours each day. CCTV surveillance at the Academy is intended for the purposes of:

- protecting the Academy buildings and Academy assets, both during and after Academy hours;
- promoting the health and safety of staff, pupils and visitors;
- preventing bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that the Academy rules are respected so that the Academy can be properly managed.

21.1 LOCATION OF CAMERAS

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. Emerson Park Academy has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

The use of CCTV to control the perimeter of the Academy buildings for security purposes has been deemed to be justified by the Governing Body. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.

CCTV Video Monitoring and Recording of Public Areas in Emerson Park Academy may include the following:

- ***Protection of Academy buildings and property:*** The building's perimeter, entrances and exits, lobbies and corridors, special storage areas and receiving areas for goods/services
- ***Monitoring of Access Control Systems:*** Monitor and record restricted access areas at entrances to buildings and other areas
- ***Verification of Security Alarms:*** Intrusion alarms, exit door controls, external alarms
- ***Video Patrol of Public Areas:*** Parking areas, front and rear security gates and traffic Control
- ***Criminal Investigations (carried out by the police):*** Robbery, burglary and theft surveillance

The Academy will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

If the Academy wishes to use images/video footage of pupils in a publication, such as the Academy website, prospectus, or recordings of Academy plays, written permission will be sought for the particular usage from the parent of the pupil.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

21.2 Notification - Signage

Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at all entrances to Emerson Park Academy.
Signage shall include the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

WARNING
CCTV cameras in operation

Images are being monitored and recorded for the purpose of crime-prevention, the prevention of anti-social behavior, the prevention of bullying, for the safety of our staff and students and for the protection of Emerson Park Academy and its property. This system will be in operation 24 hours a day, every day. These images may be passed to the police.

Appropriate locations for signage will include:

- at entrances to premises i.e. external doors, Academy gates
- reception area
- at or close to each internal camera

21.3 Storage and Retention

Section 2(1)(c)(iv) of the Data Protection Acts states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained.

The images captured by the CCTV system will be retained for a maximum of 28 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel only. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher. The Headteacher has delegated the administration of the CCTV System to the Deputy Head teacher and Site Manager. In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above (such individuals may include the police, SLT, the relevant Pastoral Leader, other members of the teaching staff, representatives of LEA, representatives of the HSE and/or the parent of a recorded student). When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

21.4 ACCESS

Any electronic equipment storing the recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to tapes/images will be maintained.

Access to the CCTV system and stored images will be restricted to authorised personnel ony.In relevant circumstances, CCTV footage may be accessed:

- By the police where Emerson Park Academy are required by law to make a report regarding the

commissionof a suspected crime; or

- Following a request by the police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on Emerson Park Academy property, or

- To the HSE and/or any other statutory body charged with child safeguarding; or

- To assist the Headteacher in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardians will be informed; or

- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to Emerson Park Academy, or

- To individuals (or their legal representatives) subject to a court order.

- To the Academy's insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

Requests by the police: Information obtained through CCTV monitoring will only be released when authorised by the Headteacher following consultation with the Governing Body. If the police request CCTV images for a specific investigation, they may require a warrant and accordingly any such request made by the police should be made in writing and the Academy should immediately seek legal advice.

Access requests: On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided also that an exemption/prohibition does not apply to the release. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. To exercise their right of access, a data subject must make an application in writing to the headteacher. The Academy may make a charge for responding to such a request and must respond **within 1 calendar month.**

Access requests can be made to the following: Designated Data Protection Officer, Emerson Park Academy, Wych Elm Road, Hornchurch. RM11 3AD.

A person should provide all the necessary information to assist Emerson Park Academy in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be handed over by the Academy.

In giving a person a copy of their data, the Academy may provide a still/series of still pictures with relevant images. However, other images of other individuals will be obscured before the data is released.

21.5 Photographs and videos

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

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.

Uses may include:

- Within Academy on notice boards and in Academy newsletter, brochures etc.
- Outside of Academy by external agencies such as the Academy photographer, newspapers,campaigns, etc
- Online on our Academy 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.

22. DATA RETENTION

Data will not be kept for longer than is necessary.

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the Academy may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

23. 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.

24. CONFIDENTIALITY

The Academy will ensure that students:

- know that teachers (and all Academy staff) cannot offer unconditional confidentially;
- are reassured that their best interests will be maintained;
- know that if confidentiality has to be broken they will be informed first, then supported as appropriate;
- are encouraged to talk to their parents/carers and provided with the necessary support;
- are informed of alternative sources of confidential help, eg. an Academy counsellor, GP or local persons' advice centre;
- are given the opportunity to agree ground rules for lessons where sensitive issues may arise;
- These should be behaviour-focused and implementation should be consistent and rigorous.

The Academy will ensure that parents/carers:

- understand the Academy's policy in relation to confidentiality;
- are made aware of the Borough's Child Protection requirements;
- are encouraged to talk to their children and that opportunities to support them in this are built into

the Academy planning.

The Academy will ensure that staff understand:

- the Academy's policy in relation to confidentiality;
- that they cannot offer unconditional confidentiality to students;
- If a student discloses information at an inappropriate time or place, the teacher must communicate the disclosure immediately to the designated Child Protection Officer, using the appropriate Child Protection procedures.
- the boundaries agreed by the Academy in relation to sensitive issues;
- the agreed procedure for recording and reporting disclosures and the nature of access to this information;
- their responsibility in maintaining confidentiality, both orally and with written information;
- that the principles of confidentiality of information applies to colleague information as well as student information.

The Headteacher and Governors should monitor:

- disclosures to staff within the agreed boundaries. (If disclosures are frequent, this may point to deficiencies in young people's awareness of, or confidence in, sources of confidential medical advice. This should be addressed in the Academy's PSHE programme);
- consistency in implementation of the policy, ensuring that boundaries are not being overstepped and new staff receive information about this policy in their induction.

Any outside agencies working with the Academy (including supply teachers) will work within an agreed framework and will complete a non-disclosure agreement for the time that they are in the Academy. Information is only shared on a 'need to know' basis. Please see Appendix 3 for an example of a non-disclosure agreement.

25. BIOMETRIC DATA

25.1 What is biometric data?

Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

The Information Commissioner considers all biometric information to be personal data as defined by the General Data Protection Regulations (GDPR) and Data Protection Act 2018; this means that it must be obtained, used and stored in accordance with these requirements (see relevant paragraphs below).

The Protection of Freedoms Act includes provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the GDPR and DPA. (See relevant section below).

Biometric data is considered by the Academy to be Special Category data and hence will be processed as such.

25.2 What is an automated biometric recognition system?

An *automated biometric recognition system* uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

Biometric recognition systems can use many kinds of physical or behavioural characteristics such as those listed in 1) above.

25.3 What does processing data mean?

The term 'Processing' is defined under the GDPR and DPA as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

An automated biometric recognition system processes data when:

a. recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
b. storing pupils' biometric information on a database system; or
c. using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

25.4 The Protection of Freedoms Act 2012

Notification and Parental Consent (Where the data are to be used as part of an automated Biometric recognition system) (see 2 above), Schools and colleges must also comply with the additional requirements in sections 26 to 28 of the **Protection of Freedoms Act 2012**.)

The written consent of at least one parent must be obtained before the data are taken from the child and used (i.e. **'processed'** – see 3 above). 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.

What the law says:

1) Schools and colleges must notify each parent of a pupil under the age of 18 if they wish to take and subsequently use the child's biometric data as part of an automated biometric recognition system.

2) As long as the child or a parent does not object, the written consent of only one parent will be required for a school or college to process the child's biometric information. A child does not have to object in writing but a parent's objection must be written.

3) Schools and colleges will not need to notify a particular parent or seek his or her consent if the School or college is satisfied that:

a. the parent cannot be found, for example, his or her whereabouts or identity is not known;
b. the parent lacks the mental capacity to object or to consent;
c. the welfare of the child requires that a particular parent is not contacted, for example where a child has been separated from an abusive parent who is not to be informed of the child's whereabouts; or
d. where it is otherwise not reasonably practicable for a particular parent to be notified or for his or her consent to be obtained.

4) Where neither of the parents of a child can be notified for one of the reasons set out above (which

would mean consent cannot be obtained from either of them), section 27 of the Protection of Freedoms Act 2012 sets out who should, in such circumstances, be notified and who can give consent:

a. if the child is being 'looked after' by a local authority or is accommodated or maintained by a voluntary organisation (i.e. a not-for-profit organisation), the local authority, or as the case may be, the voluntary organisation must be notified and their written consent obtained.
b. if paragraph (a) above does not apply, then notification must be sent to all those caring for the child and written consent must be gained from at least one carer before the child's biometric data can be processed (subject to the child and none of the carers objecting in writing). There will never be any circumstances in which a school or college can lawfully process a child's biometric information (for the purposes of using an automated biometric recognition system) without one of the persons above having given written consent.

5) Under the Education (Pupil Registration) Regulations 2006, Schools are required to keep an admissions register that includes the name and address of every person known to the Academy to be a parent of the child, including non-resident parents. Academies that wish to notify and seek consent to process a child's biometric information at any point after the enrolment of a child should have contact details for most parents in the admission register.

6) Academies should be alert to the fact that the admission register may, for some reason, not include the details of both parents. Where the name of only one parent is included in the admission register, Academies should consider whether any reasonable steps can or should be taken to ascertain the details of the other parent. For example, the Academy might ask the parent who is included in the admission register or, where the Academy is aware of local authority or other agency involvement with the child and its family, may make enquiries with the local authority or other agency. Schools and colleges are not expected to engage the services of 'people tracer' or detective agencies but are expected to take reasonable steps to locate a parent before they are able to rely on the exemption in section 27(1)(a) of the Protection of Freedoms Act (i.e. notification of a parent not required if the parent cannot be found).

7) An option would be for Schools and colleges to notify parents that they intend to take and use their child's biometric information as part of an automated biometric recognition system and seek written consent to do so at the same time as obtaining details of parents as part of the enrolment process. In other words, details of both parents would be requested by the Academy or college for both purposes (enrolment and notification of intention to process biometric information).

8) Notification sent to parents should include information about the processing of their child's biometric information that is sufficient to ensure that parents are fully informed about what is being proposed. This should include: details about the type of biometric information to be taken; how it will be used; the parents' and the pupil's right to refuse or withdraw their consent; and the Academy's duty to provide reasonable alternative arrangements for those pupils whose information cannot be processed. A suggested sample 'Notification and Consent' template is included at the end of this advice.

25.5 The pupil's right to refuse

What the law says:

If a pupil under 18 objects or refuses to participate (or to continue to participate) in activities that involve the processing of their biometric data, the School or college must ensure that the pupil's biometric data are not taken/used as part of a biometric recognition system. A pupil's objection or refusal overrides any parental consent to the processing. At Emerson Park Academy, students are

able to give their full names at the till point in order to access their account without having to use their thumb print.

Emerson Park Academy ensures that students are informed of their right to refuse through its Privacy Notices. The steps taken by Schools and colleges to inform pupils should take account of their age and level of understanding. Parents should also be told of their child's right to object or refuse and be encouraged to discuss this with their child.

All parents are asked to complete a form to confirm their consent. This is seen in Appendix 1.

26. SUBJECT ACCESS REQUESTS

Under the Data Protection Act 2018 individuals have the right to request access to information any organisation holds about them. Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the Data Protection Officer at info@emersonparkacademy.org

The Academy will not reveal the following information in response to subject access requests:

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

26.1 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request

- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if 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

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.

26.2 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the designated Data Protection Officer. If staff receive such a request, they must immediately forward it to the designated Data Protection Officer.

27. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

Parents have the right of access to their child's educational record, free of charge, within 1

calendar month of a request.

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

For students under the age of 12:

Children below the age of 12 are generally not 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 our Academy may 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.

For students aged 12 and above:

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 our Academy 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.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our Academy may not be granted without the express permission of the pupil.

28. FREEDOM OF INFORMATION

Emerson Park Academy is committed to transparency and improving accountability and fully supports the aims of the Freedom of Information Act 2000.

- The Freedom of Information Act 2000 (The Act) came into force on 1st January 2005.
- The Act provides public access to information held by public authorities and requires them to publish certain information about their activities.
- It does this in two ways:
    - Public Authorities are obliged to publish certain information about their activities; and
    - Members of the public are entitled to request information from public authorities.
- The Freedom of Information Act may work alongside other laws. These include:
    - Environmental Information Regulations 2004
    - Data Protection Act 2018
    - Infrastructure for Spatial Information in the European Community Regulations 2009
    - Access to Health Records Act 1990
    - Local Government Acts
    - Education (Pupil Information) Regulations
- The Act covers recorded information that is held, which may include printed documents, computer files, letters, emails, photographs and sound or video recordings. It does not include personal data (information regarding the individual making the request or another person) as this is covered by the Data Protection Act 2018.
- Anyone can request information by writing to the Academy (letter or email or online form) and it will be provided to them in a suitable format (subject to any exemptions that may be applied).There is no formal application procedure.
- Where the information is a data set, it should be provided in a format which is suitable

forre-use (i.e. CSV file).

Emerson Park Academy will comply with the Act in the following way:

- The Academy will ensure that systems and procedures are in place to meet all the duties set out in the Act.
- The Act covers all written requests for information received by the Academy (including emails and faxes). However, where a request is deemed to be an "ordinary" request, (usually where the information is readily available, e.g. the provision of a list of subjects taught by the Academy), this information will be provided and not logged as a Freedom of Information request.
- Where a request asks for additional information, and is more complex in nature, this will be treated as a formal Freedom of Information request and will be logged and handled under Freedom of Information procedures.
- Detailed guidance on Freedom of Information is published by the Information Commissioner's Office (ICO) and is used as the basis of the Academy's policy and procedures. A copy of the latest version of the Guide to Freedom of Information can be found on the Information Commissioner's website.
- The Academy will handle all requests for information in line with thelatest guidance issued by the Information Commissioner's office.
- This means that we will
    - Acknowledge receipt of your request promptly.
    - Identify, collect and provide the information you have requested as soon as possible and no later than **20 working days** after receipt of your request. If we do not hold the information, we will tell you.
    - Tell you if the request will incur a fee
    - Inform you of the reasons for refusing a request within **20 working days**.
    - Where we cannot provide a complete response, we will provide you with the information that we have – partial response.
    - Where the request is very broad we will contact you to ask for a more specific request
    - Keep you informed if there is a delay.
    - Undertake a review of your request if you are dissatisfied with the response or the way your request was handled.
- All staff will be made aware of their responsibilities under the Act and training will be provided where needed.

28.1 Copyright

The Act does not affect copyright and intellectual property rights that give owners the right to protect their original work against commercial exploitation by others.

When giving access to information under the Act, conditions and restrictions cannot be placed on that access. However, a copyright notice can be included with the information disclosed, and a claim can be made in the courts if the requester or someone else uses the information in breach of copyright.

The ICO encourages public authorities to use the open government licence provided by the National Archives.

The Controller of Her Majesty's Stationery Office (HMSO) has developed this licence as a tool to enable Information Providers in the public sector to license the use and re-use of their Information under a common open licence. The Controller invites public sector bodies owning their own copyright and database rights to permit the use of their Information under this licence.

28.2 Who can apply

- Anyone can make a request for information under the Freedom of Information (FOI) Act or

Environmental Information Regulations (EIR) – they do not have to be UK citizens, or resident in the UK. Freedom of Information requests (FOI) and Environmental Information Regulations (EIR) requests can also be made by organisations (i.e. newspapers, charities, campaign group or company). Employees of a public authority can also make a request.

- When a request is received, it is the Academy's responsibility to identify that a request has been made and handle it accordingly, under the correct legislation (see paragraph 1 above)

28.3 What can be requested

- The Act covers any ***recorded information*** that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. It is not limited to "official documents". Recorded information includes:
    - drafts;
    - printed documents;
    - computer files;
    - letters;
    - emails;
    - photographs;
    - sound, telephone or video recordings

- The Act does not cover information that is in someone's head, only that which is already available in a recorded form. Therefore, the Academy is not required to create new information or question staff who may know the answer.
- Public authorities include government departments, local authorities, the NHS, state Schools and police forces.
- The Act covers information that is held on behalf of a public authority even if it is not kept on the authorities' premises, for example, when public services are subcontracted to an external organisation.
- The Act does not give people access to their own personal data (information about themselves). If a member of the public wants to see information that a public authority holds about them, it will be handled as a subject access request under the Data Protection Act 2018 (DPA).

28.4 How can a request be made

- Requests for Information under the Freedom of Information Act must:
    - Be made in writing (letter, email or via online form)
    - Include the requester's real name.
    - Include an address for correspondence (it need not be residential or work address – it can be any address that can be used to contact them, and can be either postal or email).
    - Describe the information requested.
- If an applicant is unable to write their request, the authority is required to offer help and assistance; this may mean a staff member recording their verbal request in a written form on their behalf.
- Requests for "environmental information" can also be made verbally.
- When considering the requests received from the public, the Academy is required to act in favour of disclosure, unless there is a good reason not to. All requests for information must be treated equally, except under some circumstances relating to vexatious requests and personal data. The applicant does not have to give a reason for wanting the information, and all applicants should be treated equally, whether they are journalists, residents, MPs, public authority staff or foreign researchers. As a result, the Act is sometimes described as being "applicant and purpose blind".
- All information that is released should be considered as if it were being released to the world at large.
- The Academy has **20 working days** to complete this process and is also required to provide advice and assistance to any applicant who seeks to make a request or who has made a

request.

- A request for information may only be refused where a **specified exemption applies**. Even where certain exemptions apply information may still be released if it is in the public interest to do so.
- If an applicant is unhappy with a refusal, the way their request was handled or the information that was provided to them, they can ask for an internal review to be undertaken.
- If they are still not happy following the outcome of the internal review, they then have the right to take the matter up with the Information Commissioner directly, and if that complaint is upheld there will be a Decision Notice issued against the Academy. The notice will also be published on
  the ICO website.

28.5 Active publication of information

- All public authorities are required to have a publication scheme detailing the information that is routinely made available to the public, and the Information Commissioner's Office has provided a model which must be used.
- The guidance is not definitive – public authorities are expected to provide as much information as possible on a routine basis.

28.6 Handling Freedom of Information / Environmental Information Requests

- The Academy has up to **20 working days** to respond to a Freedom of Information Request, and the Information Commissioner's Office expects that a **minimum of 85%** of requests should be answered within this time - frame. However, it is considered good practice to respond to requests as soon as possible, and the Academy strives to achieve a **100%** response rate within the timeframe.
- If an applicant asks for an internal review because they are unhappy with the outcome of their request, this must be undertaken by a senior officer in the Academy who was not previously involved with the request.
- Copies of information collected for responses to Freedom of Information requests should be kept for three complete calendar years and then disposed of in accordance with the document retention schedule. Unless there is a legal/statutory reason for keeping them as hard copies, they should be kept as electronic files.

29. STORAGE OF RECORDS

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use.
- Papers containing confidential personal information should not be left on office and classroom desks, on staff room tables or pinned to noticeboards where there is general access.
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the Academy office and agree this in advance with the designated Data Protection Officer.
- Passwords that are at least 8 characters long containing letters and numbers are used to access Academy computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Encryption software/hardware 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 for Academy-owned equipment.
- 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 (see section 15)

30. DISPOSAL OF RECORDS

The Academy recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files.

Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

The Academy will always choose a qualified source for disposal of IT assets and collections.

31. TRAINING

Our staff and governors are provided with Data Protection and GDPR training as part of their induction process.

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

We have also implemented a yearly programme to train staff, SLT and Governors in all areas of Data Protection and GDPR. This training programme will be consistent, ongoing and relevant.

32. MONITORING ARRANGEMENTS

The designated DPO is responsible for monitoring and reviewing this policy.

This document will be reviewed when the General Data Protection Regulation comes into force, and then **every 2 years**.

At every review, the policy will be shared with the governing board.

Appendix A

The consent forms part of the admissions form:

- **BIOMETRIC INFORMATION CONSENT:**

Please complete & sign to indicate that you consent / do not consent to Emerson Park Academy storing information from your child's fingerprint as part of an automated biometric recognition system used for identification for the school catering services.
In giving your consent, you are authorising the Academy to use your child's biometric information for this purpose only until they leave the school.
If you wish to withdraw your consent at any time, this must be done so in writing and sent to the school at the address above.

☐ I give consent to information from the fingerprint of my child

☐ I do not consent to information from the fingerprint of my child

being stored by Emerson Park Acdemy for use as part of an automated biometric recognition system for the purpose of identification within the school. I understand that I can withdraw consent at any time in writing.

Parent/Carer's Full name:

……..

Signature: …….. Date: ……

Privacy /Fair Processing Notice

We hold personal data about pupils to support teaching and learning, to provide pastoral care and assess how the Academy is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, Local Authorities and the Department for Education.
For Further information on our procedures please refer to the 'Student Privacy Notice' on the Academy's website. If you have any questions, please email: info@emersonparkacademy.org

Appendix 2

The procedure to be followed in the event of a suspected personal data breach:

This procedure is based on guidance on personal data breaches produced by the ICO (Information Commissioner's Office).

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Academy's designated DPO (Data Protection Officer) who can be contacted at info@emersonparkacademy.org.
- The designated DPO will investigate the report, and determine whether a breach has occurred. To decide, the designated DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The designated DPO will alert the headteacher and the chair of governors
- The designated DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The designated DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The designated 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 designated 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
    - Identity 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 designated DPO must notify the ICO.

- The designated DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on a Google sheet.

- 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 designated 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 designated 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 designated 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 designated DPO expects to have further information. The designated DPO will submit the remaining information as soon as possible
- The designated DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the designated 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 designated 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 designated DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The designated DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored by the designated DPO on the GDPR Audit project documentation platform.

- The designated DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We have a full GDPR annual training programme to mitigate the occurrence of data breaches. We will also take the necessary steps to minimise the impact of the different data breaches that might occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Name: Address:

Appendix 3

Non-Disclosure Agreement

For use by Schools for casual staff (including any external agencies), contractors working outside of a contract and volunteers.

Placement period from: to:

I understand that in the course of my duties I may have access to personal and other confidential information relating to pupils, teachers, colleagues, partners and contractors.

I further understand that I must use this information for school purposes only and in accordance with the Academies policies and procedures for the use of information, which ensure legal compliance with data protection legislation.

I acknowledge that I must only pass on such identifiable information to authorised recipients, whether within or outside the Academy. If I am uncertain as to whether the recipient is authorised, I will check with my manager before passing on such information.

I acknowledge that I must not access or attempt to access any information system without the proper authorisation of my manager and then only to carry out the authorised functions.

I also acknowledge that if I breach this confidentiality, I may be liable for serious disciplinary action taken against me, up to and including exclusion. I acknowledge that in addition I may be subject to criminal prosecution under either the Data Protection Act 2018 or the Computer Misuse Act 1990 or a civil prosecution for damages by the supplier of the information.

I acknowledge also that this confidentiality must continue indefinitely and that this agreement will apply after I leave the Academy.

DECLARATION

I, _____
(Name in block capitals)

confirm that I have read the above confidentiality statement, understand it, and agree to abide by it.

_____ _____

(Signature) (Date)

_____ _____

(Signature of SIRO) (Date)

Name of SIRO: Scott McGuinness

Job title: Headteacher