**Essa Foundation Academies Trust**

**Data Protection Policy**
**(updated for General Data Protection Regulation)**
**And**
**Operational Procedures for the Trust**

# Data Protection Policy

| | |
|---|---|
| Date approved by the Board of Directors | 6 July 2018 |
| Date adopted by Essa Academy Local Governing Body | TBC |
| Date adopted by Essa Primary Local Governing Body | TBC |
| Date adopted by Essa Nursery Committee | |
| Date for review | June 2020 |

**Updates**

Issue Date: 6th June 2018
Review Date June 2020

**CONTENTS**

## THE POLICY

INTRODUCTION

Essa Foundation Academies Trust (EFAT) collects and uses personal information about staff, nursery children, pupils/ students, parents/ carers, directors and governors of the trust, and other individuals who come into contact with the trust and its academies and nursery.

This information is gathered in order to enable EFAT academies and nursery to provide education and other associated functions. In addition there may be a legal requirement to collect and use information to ensure that the trust, and its academies and nursery, complies with statutory obligations.

LEGAL FRAMEWORK

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

1. The General Data Protection Regulation (GDPR)
2. The Freedom of Information Act 2000
3. The Education (Pupil Information)(England) Regulations 2005 (as amended in 2016)
4. The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
5. The School Standards and Framework Act 1998

The Trust has a duty to be registered as a data controller with the information Commissioners Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. EFAT academies and nursery, on behalf of the Trust, also have a duty to issue a Fair Processing Notice (privacy notice) to all parents/carers that summarises the information held on nursery children and pupils/ students and their families, why it is held, and the other parties to whom it may be passed on. A fair processing notice on appointment also notifies employees, directors, governors, other volunteers and other individuals. All the policies, in their most up to date form, are available on the Trust website.

The GDPR sets out the safeguards that ensure that personal information is handled correctly regardless of how it is collected, and how it is

recorded and used (whether on paper, stored on computer, or recorded in any other format or on any other material).

The GDPR also gives people rights over their personal data. The Act applies in relation to current, past or prospective contacts with Essa Foundation Academies Trust (EFAT) and/ or its academies and nursery– and covers members, directors and governors; other volunteers, all employees; nursery children, pupils/students, parents/carers; and suppliers/ contractors.

GDPR also covers the use of biometric systems in schools/academies e.g. cashless catering systems using finger print technology.

This policy should be read in conjunction with the Trust's Freedom of Information Act Policy, as well as our privacy policies.

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.

PRINCIPLES

In accordance with the requirements outlined in the GDPR, personal data will be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. 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.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that

is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. 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.
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

ACCOUNTABILITY

EFAT has implemented appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

EFAT will provide comprehensive, clear and transparent privacy policies. These policies are available on the Trust website and are subject to regular review.

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Internal records of processing activities will include the following:

1. Name and details of the organisation
2. Purpose(s) of the processing
3. Description of the categories of individuals and personal data
4. Retention schedules
5. Categories of recipients of personal data
6. Description of technical and organisational security measures
7. Details of transfers to third parties, including documentation of the transfer mechanism safeguards in place

The Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:

1. Data minimisation

2. Pseudonymisation
3. Transparency
4. Allowing individuals to monitor processing
5. Continuously creating and improving security features
6. Data protection impact assessments will be used, where appropriate

DATA PROTECTION OFFICER (DPO)
A DPO will be appointed in order to:
1. Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
2. Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.
The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

The DPO will report to the highest level of management at the school, which is the CEO.

The DPO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

The Data Protection Officer is Mrs Kelsey. Her contact details are on the Privacy Notice.

LAWFUL PROCESSING
The legal basis for processing data will be identified and documented prior to data being processed. Details can be found in the Personal Data Log, which is held by the Trust.

Under the GDPR, data will be lawfully processed under the following conditions:
1. The consent of the data subject has been obtained.
1. Processing is necessary for:
1. Compliance with a legal obligation.

2. The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
3. For the performance of a contract with the data subject or to take steps to enter into a contract.
4. Protecting the vital interests of a data subject or another person.
5. For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

Sensitive data will only be processed under the following conditions:

1. Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
2. 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.
3. Processing relates to personal data manifestly made public by the data subject.
4. Processing is necessary for:

1. Carrying out obligations under employment, social security or social protection law, or a collective agreement.
2. Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
3. The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
4. 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.
5. 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.
6. 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.
7. Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

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 Trust ensures 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 reobtained.

Consent can be withdrawn by the individual at any time.

Where a child is under the age of 16 the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

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 school 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:

1. The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
2. The purpose of, and the legal basis for, processing the data.
3. The legitimate interests of the controller or third party.
4. Any recipient or categories of recipients of the personal data.
5. Details of transfers to third countries and the safeguards in place.
6. The retention period of criteria used to determine the retention period.

7. The existence of the data subject's rights, including the right to:
1. Withdraw consent at any time.
2. Lodge a complaint with a supervisory authority.
1. 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, 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 categories of personal data that the school holds, the source that 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:

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

ACCESS RIGHTS

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 Trust 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 Trust 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 30 days 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 Trust 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 Trust will ask the individual to specify the information the request is in relation to.

A child or young person will always be the owner of their personal information however if a young person is incapable of making their own decisions which is generally accepted as under the age of 13, The primary carer or guardian would act on their behalf. This authority is only extended to functions that are in the 'best interests' of the child or young person.

Under the Education (Pupil Information) (England) Regulations 2005, a parent has the right to access their child's educational record.

Under the Regulations, requests from parents to view their child's educational record will be dealt with by the Board of Governors. All other requests for personal information from the child, or someone acting on their behalf, will be dealt with by the Academy Head or Nursery Manager on behalf of their school.

A SAR form can be found in **Appendix 3**.

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 Trust will inform them of the rectification where possible.

Where appropriate, the Trust 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 Trust 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.

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:

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

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

1. To exercise the right of freedom of expression and information
2. To comply with a legal obligation for the performance of a public interest task or exercise of official authority
3. For public health purposes in the public interest
4. For archiving purposes in the public interest, scientific research, historical research or statistical purposes
5. 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 Trust will inform other organisations that process the personal data to erase links to and copies of the personal data in question.

THE RIGHT TO RESTRICT PROCESSING

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

In the event that processing is restricted, the Trust 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 Trust will restrict the processing of personal data in the following circumstances:

1. Where an individual contests the accuracy of the personal data, processing will be restricted until the Trust has verified the accuracy of the data
2. Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual
3. Where processing is unlawful and the individual opposes erasure and requests restriction instead
4. Where the Trust 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 Trust 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 Trust will inform individuals when a restriction on processing has been lifted.

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:

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

Personal data will be provided in a structured, commonly used and machine-readable form.

The Trust will provide the information free of charge.

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

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

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

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

Where the request is complex, or a number of requests have been received, the timeframe 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 Trust 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.

THE RIGHT TO OBJECT

The Trust 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:

1. Processing based on legitimate interests or the performance of a task in the public interest

2. Direct marketing
3. 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:

1. An individual's grounds for objecting must relate to his or her particular situation.
2. The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust 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:

1. The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
2. The Trust cannot deny an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

1. The individual must have grounds relating to their particular situation in order to exercise their right to object.
2. Where the processing of personal data is necessary for the performance of a public interest task, the school 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 Trust will offer a method for individuals to object online.

AUTOMATED DECISION MAKING AND PROFILING

Individuals have the right not to be subject to a decision when:

1. It is based on automated processing, e.g. profiling.
2. It produces a legal effect or a similarly significant effect on the individual.

The Trust will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the Trust will ensure that the appropriate safeguards are in place, including:

1. Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
2. Using appropriate mathematical or statistical procedures.

3. Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
4. Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

1. The school has the explicit consent of the individual.
2. The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS

The Trust will act in accordance with the GDPR by adopting a 'privacy by design' approach and implement technical and organisational measures which demonstrate how the Trust 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 Trust's data protection obligations and meeting individuals' expectations of privacy.

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

A DPIA will be carried out 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:

1. Systematic and extensive processing activities, such as profiling
2. Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
3. The use of CCTV.

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

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

Where a DPIA indicates high-risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

DATA BREACHES

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

The Trust leadership team will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

Procedures for identifying and reporting a data breach are included in **Appendix 1**

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

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

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 Trust 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 Trust, 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:

1. The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
2. The name and contact details of the DPO
3. An explanation of the likely consequences of the personal data breach
4. A description of the proposed measures to be taken to deal with the personal data breach

5. Where appropriate, a description of the measures taken to mitigate any possible adverse effects

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

Records will be maintained of any suspected breaches of information security using the data breach report form supplied to staff.

The form will be completed in the event of loss of unauthorised disclosure of information. The details of the incident will be used to create a correctional action plan to ensure that a similar incident does not happen again.

Following a reported incident, the Trust will investigate and, after liaising with the Local Authority, decide if the incident is of sufficient severity to report to The Information Commissioners Office.

DATA SECURITY

1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
2. Confidential paper records will not be left unattended or in clear view anywhere with general access.
3. Confidential data is not displayed on walls etc. where non-authorised staff/students/visitors can see it.

NB – display of confidential data could include student photos with name and form details.

4. Personal digital data is encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up to a separate server and an offsite backup.
5. Where personal data is saved on removable storage or a portable device, the device will be kept secured by password and/or in a locked filing cabinet, drawer or safe when not in use.
6. As per the ICT policy, memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
7. All electronic devices are password-protected to protect the information on the device in case of theft.
8. Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.
9. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
10. Staff lock their computers when they are not in the room.
11. Staff do not access confidential information on their computer when non-authorised staff /students/visitors can see the screen.

12. Attachments sent via email that containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
13. The S2S system, provided by the DfE, is used for sending confidential and personal information between schools including the Common Transfer File, updating of student details via the Learning Record Service (LRS), apply for and receive student record numbers and sending/receiving of messages between other schools in the network.
14. Emails to parents will be sent through a secure system, ensuring that recipients are unable to view email addresses of other parents.
15. When sending confidential information by fax, staff will always check that the recipient is correct before sending.
16. Staff and governors who use their work laptops, computers, iPads etc. for school purposes offsite will ensure that personal data is accessed via the School's Remote Access system or will follow the security procedures detailed below:

Security procedures - 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 adhere to the following procedures for security, i.e.:

1. The data is kept secure under lock and key.
2. Electronic devices are password protected
3. The data is kept private and not viewed in a public area or where friends/family etc. can view the data.
4. The data is returned to Trust premises or destroyed as soon as possible.
5. The data is removed from electronic devices and stored on the Trust's network as soon as possible.
6. Where staff wish to work using a cloud-based platform then the IT department must set up the required area. Personal iCloud, Google Drive accounts etc. must not be used
7. The person taking the information from the school premises accepts full responsibility for the security of the data.
8. Before sharing data, all staff members will ensure:

1. They are allowed to share it.
2. That adequate security is in place to protect it.
3. Who will receive the data is detailed in the Trust's privacy notices which can be found on the Trust website.
4. The Data Protection Officer has been informed of the data sharing.

NB – Sharing data includes saving data to online platforms such as MyMaths etc. Where any personal staff or pupil data is entered onto a system separate to the school then this is defined as sharing of data.

1. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Trust containing sensitive information are supervised at all times.
2. The physical security of the school's buildings and storage systems, and access to them, is regularly reviewed. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
3. EFAT takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
4. The ICT Manager is responsible for continuity, and recovery measures are in place to ensure the security of protected data.

A Personal Data Log will be created and maintained by the Trust, which summarises each information asset the Trust maintains.

PUBLICATION OF INFORMATION
EFAT will not publish any personal information, including photos, on its website without the permission of the affected individual.

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

PERSONAL INFORMATION TO 3RD PARTIES

**1. Information sharing with professionals working with children**

Information sharing between professionals is vital to ensure the wellbeing of children. The Trust will follow the '7 golden rules of Information Sharing' described by the DfE:

1. Remember that the GDPR is not a barrier to sharing information
2. Be open and honest with the person or family
3. Seek advice if you are in any doubt
4. Share with consent where appropriate
5. Consider safety and well-being
6. Necessary, proportionate, relevant, accurate timely, and secure
7. Keep a record of your decision and reasons
8. Unauthorised disclosure of personal data is a criminal offence and will likely lead to disciplinary action

**b. Investigation of a crime**

The Trust will treat requests for information from an official bodies related to criminal or taxation purposes under The Law Enforcement Directive. The Trust requires the requestor to complete the Request for Personal Data form (**Appendix 2**).

Requests from the police will be countersigned by a person no lower than inspector. For requests from other organisations other than the police, the form will be countersigned by a person of a higher position within the organisation than the person making the request.

The decision regarding access will be made by the Principal or the CEO. Generally, the Trust reserves the right not to release the data but there may be situations such as the receipt of a court order that requires the Trust to release the information.

CCTV AND PHOTOGRAPHY

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

The Trust notifies all students/pupils, staff and visitors of the purpose for collecting CCTV images via notices within Trust buildings.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for six months for security purposes; the Site Manager is responsible for keeping the records secure and allowing access.

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

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

Precautions are taken when publishing photographs of pupils, in print, video or on the Trust websites.

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

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 school 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 placed in the secure shredding disposal bins, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

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.

DISCLOSURE OF NON - PERSONAL INFORMATION / FOI REQUESTS
The Trust as a public authority is subject to The Freedom of Information Act 2000, and all requests for information that is not personal information must be treated as a Freedom of Information request. FOI requests must be fully responded to within 20 (school) working days by law. The information will be provided unless the Trust can provide an exemption under the FOI act.

POLICY REVIEW
The Data Protection Officer, the Trust SLT and the governors review this policy every two years.

The next scheduled review date for this policy is **May 2020**.

APPENDIX 1

Data Breach Flowchart

The Trust should consider the below table when considering whether to recommend if a potential data breach investigation should result in the recording of a formal data breach.

| | | | | | | |
|---|---|---|---|---|---|---|
| Number of People involved | 1000+ | | | | | |
| | 100 | | | | | |
| | 50 | | | | | |
| | 5 | | | | | |
| | 1 | | | | | |
| | | e.g. Name, address | e.g. National Insurance number | e.g. Bank details, medical information | e.g. Details of a vulnerable child. | e.g Full medical files or criminal file |
| | Sensitivity of the Information | | | | | |
| Key | **Unlikely to require recommending as a formal breach** | | **Consideration should be given to recommending as a formal breach** | | **Likely to require recommending as a formal breach** | |

This table is only a guide, and the risk of harm to the individuals involved should be considered as the determining factor.

What to do if there is a data breach:

**1.** Complete the data breach report form provided in staff areas. **This needs to be completed as soon as a breach has been identified, particularly if it is likely to result in a formal data breach. The Trust is required to report serious data breaches within 72 hours.** It should be sent/given to the Data Protection Officer, the principal and the CEO.

2. Has the breach been contained?

1. If yes, this is a 'near miss' – review systems to see if there can be steps taken to reduce the possibility of further breaches

1. If the breach has not been contained, follow the safeguarding procedures if there are any risks to data subjects. If a pupil is potentially in danger from the breach, their safety is a priority and they must be protected. Follow safeguarding procedures. Once they are safe, then an investigation can commence.

2. Follow the data breach template and complete the investigation

3. Does this meet data subject notification criteria?

1. If yes, notify the subjects

1. Is this a formal breach?

1. If not, there is no further action, however systems should be reviewed to minimise risk

1. If yes, and is also a serious breach then the ICO need to be informed.
1. All **serious** breaches need to be reported to the ICO. The DPO and/or SLT will decide what needs to be reported.

APPENDIX 2

Essa Foundation Academies Trust

**Request for Personal Data Form**

| **To** |
|---|

**Details of applicant**

| | |
|---|---|
| **Name of applicant** | |
| **Job title** | |
| **Department and Section** | |
| **Full Address** | |
| **Telephone number** | |
| **E-mail address or fax number** | |
| **Investigation reference / Operation Name** | |
| **Date** | |

**Details of application**

| **1. This request is made pursuant to the Law Enforcement Directive. I can confirm that this request complies with the following non-disclosure provisions** |
|---|
| Section 29<br><br>☐ The data is necessary for the prevention or detection of crime<br><br>☐ The data is necessary for the apprehension or prosecution of offenders<br><br>Section 35<br><br>☐ The data is necessary for the purpose of or in connection with present legal proceedings<br><br>☐ The data is necessary for the purpose of or in connection with prospective legal proceedings |

| | |
|---|---|
| **2.** | **I require the following information** |
| | |
| **3.** | **Why I require the information** |
| | |
| **4.** | **What statutory powers does the requester have to demand the information** |
| | |
| ***5.*** | **I can confirm that the information you provide will be held in the strictest confidence and will not be further processed beyond the purpose for which it was requested.**<br><br>**I have grounds believing that failure to disclose the required information will be likely to prejudice my enquiries and can confirm that the details supplied on this form are, to the best of my knowledge, correct.**<br><br>**I am aware of the provisions of Law Enforcement Directive, regarding the unlawful obtaining of personal details.** |
| Signature<br><br>Print | Name |

APPENDIX 3

## Essa Foundation Academies Trust
## Subject Access Request Form

The General Data Protection Regulations (GDPR) provides you, the data subject, with a right to receive a copy of the data/information we

hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to see your data. You will also need to provide **proof of your identity.** Your request will be processed within 30 calendar days upon receipt of a fully completed form and proof of identity.

**PROOF OF IDENTITY**

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of two documents such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g. bank statement, recent utilities bill or council tax bill. The documents should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

**ADMINISTRATION FEE**

We do not generally charge for Subject Access Requests.

**Section 1**

Please fill in your details (the data subject). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

| |
|---|
| **Title:** |
| **Surname/Family Name:** |
| **First Name(s)/Forenames:** |
| **Date of Birth:** |
| **Address:**<br><br><br>**Postcode:** |
| **Previous Addresses:**<br><br>**Post Code:** |
| **Day Time Telephone Number** |

| |
|---|
| I am enclosing copies as proof of identity:<br>Birth Certificate ☐ Driving Licence ☐ Passport ☐ An official letter to my address ☐ |
| Personal Information<br>If you want to know what information is held in specific records please indicate in the box below.<br>Please tell us if you know in what capacity the information is held, together with any names or dates you have. |
| Details: |

| |
|---|
| Employment records<br>If you are a current or previous employee of Essa Foundation |

| |
|---|
| Academies Trust and are seeking personal information in relation to your employment please provide details of your role and dates of employment. |

**Section 2**

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e. the data subject).
If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

| |
|---|
| Title |
| Surname/Family Name: |
| First Name(s)/Forenames: |
| Date of Birth: |
| Address:<br><br>Postcode: |
| Day Time Telephone Number: |

| |
|---|
| I am enclosing copies as proof of identity:<br>Birth Certificate ☐ Driving Licence ☐ Passport ☐ An official letter to my address ☐ |
| What is your relationship to the data subject? (e.g. parent, carer, legal representative) |

| |
|---|
| I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:<br>Letter of authority ☐<br>Lasting or Enduring Power of Attorney ☐<br>Evidence of parental responsibility ☐<br>Other (give details): |
| Data Subject declaration:<br>I certify that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that Essa Foundation Academies Trust is obliged to confirm proof of identity/authority and it may be necessary to obtain further information in order to comply with this subject access request. |
| Name: |

| | |
|---|---|
| Signature: | Date: |

| | |
|---|---|

Warning: a person who unlawfully obtains or attempts to obtain data is guilty of a criminal offence and is liable to prosecution.

I wish to:
Receive the information in electronic form * ☐

Receive the information by post ☐

Collect the information in person ☐

View a copy of the information only ☐

Go through the information with a member of staff ☐

* Some files may be too large to transmit electronically and we may have to supply in CD format)
** Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'. It is recommended

**Please send your completed form and proof of identity to:**

Kirsty Kelsey, Data Protection Officer
Essa Foundation Academies Trust
Lever Edge Lane
Bolton
BL3 3HH
**kelseyk@essaacademy.org**