Eastwood Park Academy Trust



Data Protection Policy

|  |  |
| --- | --- |
| Author’s Name:  | Mr. N. Houchen |
| Date Reviewed | June 2017 |
| Date Ratified by Trust |  |
|  |  |
| Signature of CEO |  |
| Signature of Chair of Trust |  |

Contents

[1.0 Purpose 3](#_Toc481150485)

[2.0 Principles of the Data Protection Act 1998 3](#_Toc481150486)

[3.0 How the Trust will abide by the DPA 3](#_Toc481150487)

[4.1 Board of Trustees 4](#_Toc481150488)

[4.2 CEO 4](#_Toc481150489)

[4.3 Principal 4](#_Toc481150490)

[4.4 Trust Staff 4](#_Toc481150491)

[5.0 Data Processing 4](#_Toc481150492)

[5.1 Personal Data Held 4](#_Toc481150493)

[5.2 Security of Personal Data 5](#_Toc481150494)

[5.3 External Data Processing 5](#_Toc481150495)

[5.4 Sensitive and High Risk Personal Data 5](#_Toc481150496)

[5.5 Medical Records 6](#_Toc481150497)

[5.6 Staff Records and the Monitoring of Staff 6](#_Toc481150498)

[5.7 CCTV Monitoring 6](#_Toc481150499)

[5.8 Recording of Telephone Calls 6](#_Toc481150500)

[5.9 Publication of Personal Data 7](#_Toc481150501)

[5.10 Retention and Disposal of Data 7](#_Toc481150502)

[6.0 Access to Data and Disclosure 7](#_Toc481150503)

[6.1 Data Subjects Rights 7](#_Toc481150504)

[6.2 Sharing Information 8](#_Toc481150505)

[7.0 Use of Personal Information/Images 8](#_Toc481150506)

[8.0 Privacy Notice 8](#_Toc481150507)

[Appendix A - Use of Personal Information/Images Notice 9](#_Toc481150508)

[Appendix B - Privacy Notice 10](#_Toc481150509)

# 1.0 Purpose

The purpose of this policy is to ensure that the Trust and people working in it are aware of their obligations under the Data Protection Act 1998 (DPA).

# 2.0 Principles of the Data Protection Act 1998

The Trust has a duty to comply with the 8 principles of the DPA, as summarised below.

Personal information should be:

* Fairly and lawfully processed.
* Only obtained for specified purposes and not processed for any other purpose which is incompatible with that.
* Adequate, relevant and not excessive.
* Accurate and up-to-date.
* Not kept for any longer than is necessary.
* Processed in line with the rights afforded to individuals under the legislation, including the right of subject access requests.
* Kept secure.
* Not transferred to countries outside the European Economic Area (EEA) without adequate protection.

# 3.0 How the Trust will abide by the DPA

 The Trust will:

* Process personal information only where it is strictly necessary for legitimate purposes.
* Collect only the minimum personal information required for those purposes. It will not process excessive personal information.
* Provide clear information to individuals about how their personal information will be used and by whom.
* Only process relevant and adequate personal information.
* Process personal information fairly and lawfully.
* Maintain an inventory of the categories of personal information processed by the constituent academy.
* Keep personal information accurate and, where necessary, up-to-date.
* Retain personal information only for as long as is necessary for legal or regulatory reasons or legitimate purposes.
* Respect individuals’ rights in relation to their personal information, including their rights of subject access e.g. subject access requests.
* Keep all personal information, in whatever format, secure.
* Only transfer personal information outside the EEA in circumstances where it can be adequately protected.
* Only apply the exemptions applicable under information legislation.
* Have a regular review and audit of the way personal information is held, managed and used and ensure methods of handling personal information are regularly assessed and evaluated.
* Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
* Have clear procedures for responding to requests for information.
* Acknowledge, investigate and fully respond to all complaints relating to a request for information according to the Trust’s Complaints Policy.

**4.0 Responsibility and Accountability for Data Protection**

## 4.1 Trust

The Trust has overall responsibility for all constituent academies. The Trust, as a corporate body, is the ‘Data Controller’.

## 4.2 CEO

The CEO works with constituent academies to ensure compliancy with the DPA.

## 4.3 Principal

The Principal in each constituent academy has responsibility for:

* Managing its information and records properly and complying with all the relevant legislation.
* Complying with this policy.
* Approving procedures where personal information is processed such as: the management and communication of privacy notices; handling of subject access requests from individuals; the collection and handling of personal information; complaints handling; management of personal information security incidents; and outsourcing and off-shoring of personal information processing.

## 4.4 Trust Staff

Staff should not process any personal data unless they are authorised to do so. Further, they should not knowingly or recklessly obtain or disclose personal data and, in such instances, may be subject to the Trust’s Disciplinary Misconduct Policy.

# 5.0 Data Processing

## 5.1 Personal Data Held

The Trust will maintain an inventory of all the categories of personal information that it holds and the reasons for holding that data. Such inventories will be reviewed and updated annually and any changes communicated to the Data Protection Officer for the Trust, Mr. C. Niner.

Personal data is defined as any combination of items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

* Personal information about members of the Trust community - pupils, members of staff, parents/carers, names, addresses, contact details, legal guardianship contact details, health records, disciplinary records etc.
* Curricular data - class lists, pupil progress records and reports.
* Employment records - history, taxation, NI, pension, PM appraisal, references etc.
* Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

## 5.2 Security of Personal Data

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

All staff are responsible for ensuring that:

* Any personal data which they hold is kept securely.
* Personal information is not disclosed either orally, in writing, electronically or otherwise to any unauthorised person.

Personal information should be:

If a hard copy:

* Not left accessible to unauthorised persons.
* Preferably, and where possible, kept in a locked filing cabinet or in a locked drawer.
* Disposed of as confidential waste.

If electronic:

* Be password protected\* or kept only on portable media which is itself secure.
* Where practicable, held on a PC with ‘time out’ facility and/or where SIMS is closed down daily.
* Be deleted in accordance with corporate retention periods and evidence of such deletion recorded to provide for necessary audit trails.

**\*Passwords should be at least eight characters long and include at least one number and one special character with a 30 day prompt to change passwords.**

Every electronic system that holds personal information has a designated manager who has overall responsible for controlling access to and the information security of that system. Advice on making personal data secure is provided by the Data Protection Officer.

Any incidents where personal data has been lost or disclosed to unauthorised recipients should be immediately reported to the Principal who will advise what action should be taken to mitigate the damage.

## 5.3 External Data Processing

All contracts with third-party providers, where the processing of personal data is required, shall include a requirement for the contractor to comply with the requirements of the DPA.

## 5.4 Sensitive and High Risk Personal Data

Sensitive personal data is defined in the DPA as information concerning an individual’s:

* Racial or ethnic origin.
* Political opinions.
* Religious beliefs or other beliefs of a similar nature.
* Trade union membership.
* Physical or mental health or condition.
* Sexual life.
* Criminal convictions or alleged offences.

Extra care must be taken when processing sensitive personal data as additional requirements under the DPA must be met to ensure that the processing is legitimate and safe. The advice of the Principal should be sought before any new processing of sensitive personal data commences.

There is also some personal information which is regarded as high risk and therefore a risk assessment should be carried out and additional security precautions should be implemented before processing such information.

High risk personal information includes, but is not limited to:

* Personal bank account and other financial information.
* National identifiers, such as NI numbers.
* Personal information relating to vulnerable adults and children.
* Detailed profiles of individuals.
* Sensitive negotiations which could adversely affect individuals.
* Large numbers of records containing personal information.

## 5.5 Medical Records

These are classed as sensitive personal data under the DPA, and, therefore, additional care should be taken when processing this information. In particular, before disclosing the medical records of anyone as part of a Subject Access Request, the advice of the relevant medical practitioner and the Principal must be sought as to whether the information should be released or not.

## 5.6 Staff Records and the Monitoring of Staff

The Trust will endeavour to comply with the ICO’s employment practices code in relation to the processing of staff personal information. This Code exemplifies good practice and strikes a balance between the legitimate expectations of workers that personal information about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own businesses.

## 5.7 CCTV Monitoring

CCTV monitoring is undertaken using software called Qvis Viewer and is carried out in accordance with the ICO’s code of practice on CCTV.

## 5.8 Recording of Telephone Calls

Currently the Trust does not record phone calls as a matter of standard practice. However, should this occur, the individual must be advised what information is being recorded, the reasons for recording the information, whether the information will be shared with anyone else and, if so, whom it will be shared with and for how long the information will be retained.

## 5.9 Publication of Personal Data

Personal data should generally only be made public if there is a legal or statutory requirement to do so. On occasion, it may be appropriate to publish personal information with the individual’s consent. However, in such cases staff must ensure that the consent is freely given. Staff must also be aware that it is possible to withdraw consent at any time and, if that happens, publication of the data must cease immediately.

## 5.10 Retention and Disposal of Data

It is the responsibility of Trust to ensure that the information they hold is kept accurate and up-to-date and is not held for any longer than is necessary for the purpose for which it was collected.

When the data is no longer required, it should be disposed of safely. Usually pupil documentation/staff files are kept for 7 years (unless otherwise specified) after leaving the constituent academy. Advice on determining retention periods and disposing of data can will be obtained from the Information and Records Management Society.

# 6.0 Access to Data and Disclosure

## 6.1 Data Subjects Rights

The Trust will ensure that the rights of people about whom information is held, can be fully exercised under the DPA. These include:

* The right to be informed that processing is being undertaken.
* The right of access to one’s personal information.
* The right to prevent processing in certain circumstances.
* The right to correct, rectify, block or erase information which is regarded as wrong information.

If individuals do require to see their personal data, unless special arrangements already exist to allow them access to the data, they should be encouraged to make a request in writing to the Principal. He/she will reply within 40 days. If in doubt, the Principal will take the recommended view that it is better not to release the information as it can always be released at a later date with little harm, whereas if released in error it cannot easily be recovered.

On occasion, individuals give consent for the processing of their personal information. Staff must ensure that any consent given for the processing of personal information is fully informed and freely given and that individuals are aware that they may withdraw consent at any time and what the consequences would be if they withdrew their consent.

It is advisable not to rely on consent for the processing of personal data if there is another legitimate criterion for processing which could be applied. Before relying on consent, the Trust will consider the implications should individuals refuse or withdraw consent.

If it is deemed that the consent of individuals is necessary, staff should be aware that, in the case of sensitive personal data, individuals have to give explicitconsent to the processing. It is therefore good practice to obtain written consent in such cases and the Trust will aim to do this, where possible.

Requests from external organisations or third parties for personal information about individuals should be passed to the Principal (who may consult the Trust’s HR advisers – Essex Schools HR). Under no circumstances should any personal information about any individual be passed outside the constituent academy without the authority of the Principal.

## 6.2 Sharing Information

Before sharing personal information internally, it is the responsibility of individual members of staff to ensure that they have the authority to do so and that the recipient is authorised to receive such information. Failure to do so could lead to action under the Trust's Disciplinary Misconduct Policy (and, in exceptional circumstances, in criminal charges). If there is any doubt, individuals should seek the advice of the Principal.

In emails staff should aim to use pupils’ initials and year group as identification in a subject box. They should send personal information only to the relevant subject and pastoral staff.

There are occasional instances where information is shared with partners or outside organisations through agreement.

Each agreement, as a minimum, must clearly state the information that will be shared, the purposes for sharing, the basis on which sharing is carried out and the responsibilities for handling and maintaining the personal data.

# 7.0 Use of Personal Information/Images

In compliance with the fair processing requirements of the DPA, the Trust will inform parents of the data they collect, process and hold, the purposes for which the data is held and any third parties to whom it may be passed **(Appendix A).**

# 8.0 Privacy Notice

Parents are provided with a Privacy Notice at the start of every academic year which is published on constituent academies’ websites **(Appendix B).**

# Appendix A - Use of Personal Information/Images Notice

It is requirement under the Data Protection Act (DPA) that the personal data held about pupils must only be used for specific purposes allowed by law. The personal data includes: contact details, assessment/examination results, attendance information, and characteristics such as ethnic group, special educational needs, any relevant medical information, photographs and CCTV for security and safety issues.

The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the Trust as a whole is doing, together with any other uses normally associated with this provision in a school environment.

The Trust may make use of limited personal data relating to pupils, their parents or guardians for fundraising, marketing or promotional purposes. In particular, the Trust may:

* Transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the Trust.
* Make use of photographs and video of pupils in Trust publications and on the Trust and constituent academies’ websites.
* Disclose photographs and names of pupils to the media (or allow the media to take photographs or video pupils) for promotional, training and congratulatory purposes, where a pupil may be identified by name when the image is published e.g. where a pupil has won an award or has otherwise excelled.
* Make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities.
* Keep a pupil’s previous school informed of his/her academic progress and achievements e.g. sending a copy of reports for the pupil’s first year at a constituent academy to his/her previous school.

Photographs, with names identifying pupils, will not be published on the Academy website without the express permission of the appropriate individual.

Any wish to limit or object to any use of personal data should be notified to the Principal, in writing, which will be acknowledged by the constituent academy.

Parents who do not want their child’s photograph or image to appear in any of the Trust’s promotional material, or be otherwise published, must also make sure their child knows this. **If the Trust does not receive any written objection, then it will presume your acceptance of this notice.**

Parents and pupils should be aware that where photographs or other image recordings are taken by family members or friends for personal use, the DPA will not apply e.g. where a parent takes a video of their child and some friends taking part in Sports Day.

# Appendix B - Privacy Notice

**Eastwood Park Academy Trust** is the Data Controller for the purposes of the Data Protection Act (DPA).

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school, local authority and/or the Department for Education (DfE).

We use this personal data to:

* Support our pupils’ learning.
* Monitor and report on their progress.
* Provide appropriate pastoral care.
* Assess the quality of our services.

This information will include their contact details, National Curriculum assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics such as their ethnic group, any special educational needs they may have as well as relevant medical information. For pupils enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about your learning or qualifications.

Once our pupils reach the age of 13, the law requires us to pass on certain information to Southend Local Authority who have responsibilities in relation to the education or training of 13-19 year olds. We may also share certain personal data relating to children aged 16 and over with post-16 education and training providers in order to secure appropriate services for them. A parent/guardian can request that **only** their child’s name, address and date of birth be passed to Southend Local Authority by informing the Data Protection Officer for the Trust, Mr. C. Niner. This right is transferred to the child once he/she reaches the age 16. For more information about services for young people, please go to <http://www.southend.gov.uk/>

We will not give information about our pupils to anyone without your consent unless the law and our policies allow us to do so. If you want to receive a copy of the information about your son/daughter that we hold, please contact the Data Protection Officer for the Trust, Mr. C. Niner, CNiner@eastwood.southend.sch.uk

We are required, by law, to pass some information about our pupils to the Department for Education (DfE). This information will, in turn, then be made available for use by Southend LA.

The DfE may also share pupil level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the DPA. Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to pupil level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit: <https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract>

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

If you need more information about how Southend LA and/or DfE collect and use your information, please visit:

Southend LA: <http://www.southend.gov.uk/>

The DfE: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>