Eastwood Park Academy Trust (EPAT)

EPAT

Believe Succeed Together

Data Protection Policy

Date Reviewed	June 2018
Date Ratified by Trust	July 2018

Contents

1. Aims

The Trust aims to ensure that all personal data collected about staff, pupils, parents, Members, Trustees, Local Governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

2. Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects 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, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials). • Identification number. • Location data. • Online identifier, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special Categories of Personal Data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin. • Political opinions. • Religious or philosophical beliefs. • Trade union membership. • Genetics. • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes. • Health – physical or mental. • Sex life or sexual orientation.
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

The Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and Responsibilities

This policy applies to **all staff** employed by the Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action under the Trust's Disciplinary (Misconduct) Policy.

5.1 Board of Trustees

Trustees have overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

5.2 SIRO

The Principal acts as the representative of the data controller on a day-to-day basis and the Senior Information Risk Owner (SIRO). Refer to the role profile in **Appendix 1.**

5.3 Data Protection Officer

The Data Protection Officer (DPO) for the Trust is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will provide an annual report of their activities and, where relevant, provide advice and recommendations on data protection issues.

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

The Trust's DPO is Lauri Almond and is contactable via igs@essex.gov.uk and 03330 322970.

Refer to the role profile in **Appendix 2.**

5.4 Information Champions

Information Champions (IC) play a key role in ensuring that the organisation maintains an effective framework for managing information, enabling business needs to be met within an agile and flexible environment and allowing us to work closely with partners, exchanging information legally, safely and securely.

The IC with overall responsibility for defined areas are listed in the table below.

Area	The Eastwood Academy	Bournemouth Park Academy
Overall Data and Security	Mr. C. Niner	Mr. R. Thomas
Staff Data	Mr. S. Sterling	Ms L. Sewell
Pupil Data and Safeguarding	Mr. D. Piercy	Ms L. Sewell
Governance	Mrs. K. Toms	Mrs. K. Toms

Refer to the role profile in **Appendix 3.**

5.4 All staff

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the Trust of any changes to their personal data, such as a change of address.
- Contacting the 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. Data Protection Principles

The GDPR is based on data protection principles that the Trust must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the Trust aims to comply with these principles.

7. Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

The Trust 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 school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school 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 school, 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 school 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

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

If the Trust offers online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

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

7.2 Limitation, Minimisation and Accuracy

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

If the Trust wants 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 Trust's Records Retention Policy

8. Sharing Personal Data

The Trust 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.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
  - 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.

We will also share personal data with law enforcement and government bodies where we are legally required 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.

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

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

9. Subject Access Requests

9.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school 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, email or fax to the DPO. They should include:

- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and Subject Access Requests

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.

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 a primary school academy in the Trust 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.

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 a secondary school academy in the Trust 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.

9.3 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.

9.4 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 (see section 7), 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental Requests to see their Child's Educational Record

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

11. Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it (refer to **Appendix 7 and Appendix 8**).

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around Trust sites to ensure they remain safe. We will adhere to the ICO's code of practice for the use of CCTV.

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

Any enquiries about the CCTV system should be directed to the Principal of the academy.

13. Photographs and Videos

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

We will obtain written consent from parents/carers, for photographs and videos to be taken of pupils – refer to – **Appendix 7.**

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.

14. Data Protection by Design and Default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
  For the benefit of data subjects, making available the name and contact details of the academy and DPO and all information we are required to share about how we use and process their personal data (refer to the Privacy Notices - **Appendix 5 and Appendix 6**).
  For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

15. Data Security and Storage of Records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must gain permission from their line manager.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils should change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils, Members, Trustees and Local Governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-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 (refer to section 8).

16. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it e.g. we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Refer to the Trust's Records Retention Policy

17. Personal Data Breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in **Appendix 4.**

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

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

18. Training and Monitoring

All staff, Members, Trustees and Local Governors are provided with data protection training as part of their induction process.

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

The DPO is responsible for monitoring and reviewing this policy on an annual basis.

Appendix 1: Data Protection Officer (DPO) Role Profile

Role

This role is aligned to the implementation of the requirements of one of the biggest changes to Information Laws since the introduction of Freedom of Information Laws in 2000. The General Data Protection Regulation (2016) (GDPR) requires entities that process Personal Data to have a series of controls and processes in place. One of these requirements, as outlined in Articles 37-39 of the Regulation, is to have a defined Data Protection Officer for the organisation.

The Data Protection Officer will be responsible for advising and monitoring the business's compliance with the GDPR, including performance of other formal duties as defined by the GDPR.

The Data Protection Officer applies knowledge and experience to assist the organisation in delivering services to both internal and external customers.

Key Accountabilities

- Working with the organisation to ensure compliance with their obligations under the General Data Protection Regulation and any relevant UK legislation.
- Working with organisation to monitor compliance with the Regulation, with relevant supporting UK legislation and with relevant organisational policies in relation to the protection of personal data.
- Report on the status of compliance with the Regulation to the Leadership Team and other stakeholder scrutiny groups, including briefing on specific matters for their review.
- Working with the organisation to oversee and assist in staff awareness-raising and training both online and face to face where required.
- Acting as a key stakeholder for any and all Data Protection related audits and compliance reviews, completed both internally and externally.
- Working with the organisation to provide advice and review of data protection impact assessments where required and monitoring their ongoing implementation and review. This includes acting as the formal sign off of any assessments meeting the criteria.
- Working with the organisation to investigate and process adverse incidents ensuring that any incidents that require notification to the Data Subject and/ or Supervisory Authority are completed within the 72 hour timeframe.
- Working with the organisation to advise on any Information Sharing Protocols looking to be established and shared as part of the organisation's membership of the Whole Essex Information Sharing Framework (WEISF).
- Cooperate with the Supervisory Authority (currently the Information Commissioner's Office).
- Act as the contact point for the supervisory authority on issues relating to the organisation processing of Personal Data and compliance with the GDPR and working with the organisation to resolve these.
- Act as the contact point for data subjects on issues and queries relating to the organisation's processing of Personal Data and compliance with the GDPR and working with the organisation to resolve these.
- Lead on any prior consultation needed with the supervisory authority for any organisational processing of Personal Data where required and to support the organisation and supervisory authority in this process.
- Liaise with the Leadership Team regarding Data Protection & any other information governance matters.
- Develop and maintain own skills and expertise to keep up with current requirements of the Regulation and supporting legislation.
- Build strong relationships with other Data Protection Officers to encourage the sharing of knowledge, best practice and reliable information sharing arrangements.

Knowledge, Skills and Experience

- Strong knowledge of Data Protection legislation, specifically the General Data Protection Regulation 2016 and any supporting legislation.
- Practical knowledge of Data Protection compliance including best practice.
- Experience working with Data Protection in the Public Sector or experience working with complex legal matters and being able to decipher them simply for other audiences.
- Relevant qualifications in Data Protection Law and/or Information Law / Information Governance that covers the General Data Protection Regulation 2016.
- Understanding of Information Risk Management including horizon scanning for emerging risks, reporting and analysis and route cause analysis.
- Good communication and interpersonal skills in order to liaise with staff at all levels, including Board level, and build lasting and productive relationships with internal and external stakeholders.

Appendix 2: Senior Information Risk Officer (SIRO) Role Profile

Role

- The role of the Senior Information Risk Owner (SIRO) was created to provide board-level accountability and greater assurance that information risks are addressed. The SIRO ensures that information risks are treated as a priority for business outcomes. The SIRO also plays a vital role in getting their organisation to recognise the value of its information enabling them to use it effectively.
- The SIRO as an executive-level champion: Information assets are integral to the functioning of any modern business and essential to delivering corporate objectives. By understanding, addressing and capitalising on the risks and facing an organisation's information assets, a SIRO can ensure services are delivered efficiently and with greater value for money.
- The SIRO as a champion of governance: The SIRO role is an integral part of any organisation's Information Governance Framework. As the SIRO is accountable to the Executive for risks they should actively work with relevant experts and other organisations to determine the most effective and proportionate information control measures.
- The SIRO as a champion for cultural change: The SIRO plays a pivotal role in championing a culture which is resilient, adaptable and open to change in order to effectively deliver business priorities.

Key Accountabilities

- As SIRO, you manage information risk from a business not a technical perspective.
- You focus on the strategic information risks related to the delivery of corporate objectives. This means you take a holistic approach to information risk across the supply chain and manage it in line with the organisation's risk appetite.
- To achieve this, you work with the Leadership Team to:
  Establish an information risk strategy which allows assets to be exploited and risks to be managed effectively.
  Identify business-critical information assets and set objectives, priorities and plans to maximise the use of information as a business asset
  Establish and maintain an appropriate risk appetite with proportionate risk boundaries and tolerances.
- You also work with your colleagues inside and outside your organisation to:
  - Establish an effective Information Governance Framework.
  - Act as the champion for information risk within your organisation, being an exemplar for all staff and encouraging the Leadership Team to do likewise.
  - Build networks with peers and organisations that can provide essential support and knowledge exchange services.
  - Ensure compliance with regulatory, statutory and organisational information security policies and standards.
  - Ensure all staff are aware of the necessity for information assurance and of the risks affecting the organisation's corporate information.
  - Establish a reporting and learning culture to allow the organisation to understand where problems exist and develop strategies (policies, procedures and awareness campaigns) to prevent problems occurring in the future.

Knowledge, Skills and Experience

- Strong knowledge of information legislation and best practice.
- Experience of working with information legislation and risk management in the Public Sector.
- Relevant qualifications in Information Law / Information Governance / Risk Management.
- Understanding of Information Risk Management including horizon scanning for emerging risks, and route cause analysis.
- Good communication and interpersonal skills in order to liaise with staff at all levels, including Leadership level, and build lasting and productive relationships with internal and external stakeholders.

Appendix 3: Information Champion (IC) Role Profile

Role

Information Champions play a key role in ensuring that the organisation maintains an effective framework for managing information, enabling business needs to be met within an agile and flexible environment and allowing us to work closely with partners, exchanging information legally, safely and securely.

Information Champions recommend to the Leadership Team decisions on policy or procedural issues. Individually they consider the practical effects of business practices, proposals for new or changed policies, standards, procedures and guidance focussed on the management or handling of information then, and jointly, make recommendations to the Leadership Team. They also address concerns about, and support their function in, the application of the Information Governance framework to encourage compliance with information-related legislation and regulations.

They provide appropriate support to the Leadership Team to facilitate compliance across the function with information-related legislation and regulations including, but not limited to, the Data Protection Act 1998, the General Data Protection Regulations 2016, the Human Rights Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004, Caldicott Principles and the Department of Health's Information Governance Initiative.

Key Accountabilities

- Play a key role in the Board ensuring that the Leadership Team and all other stakeholders have the relevant information about their function to inform their decisions by:
  - Attending Board meetings.
  - Considering the effect of proposals for new or changed policies, standards, procedures and guidance focussed on the management or handling of information.
  - Reflecting on aspects that are relevant to functions business practices and feeding back issues or confirming acceptability of proposals.
- Where relevant, represent own service in a specialist advisory capacity to the Board, for example, providing ad-hoc audit, HR, ICT, legal, media or records management advice at Board meetings.
- Support the Leadership Team in embedding effective information management, encouraging the pragmatic assessment of information security as an integral part of day to day operations and business change initiatives by:
  - Raising awareness, providing informed advice and actively encouraging employees to meet their responsibilities defined in our policies, supporting standards and procedures.
  - Motivating employees and gaining their commitment to the principles of the policy and relevant legislated and other information requirements.
  - Encouraging employees' attendance at relevant training.
  - Liaising with other Information Champions across the organisation to respond to cross-cutting requests for information.
  - Supporting and contributing to reviews of compliance with policy in response to complaints relating to the way information has been handled.
- Co-ordinate compliance with our procedures for responding to requests for information (in accordance with FOI and EIR) and requests for access to customers'/employees' personal files (in accordance with DPA), directing requests to appropriate teams, supporting the application of exemptions/redactions whenever information is withheld and quality assuring responses to ensure that they address the request and contain any centrally agreed wording.
- Ensure that investigations are undertaken in accordance with all relevant guidance providing support to such where required, and that mitigation strategies are implemented when security incidents or other breaches of relevant policy, standards or procedures occur within their function.
- Overseeing requests for exceptions to policy within their function, ensuring that the business justification is well documented prior to consideration, signoff and submission.

- Promote the maintenance of central information sources such as the Information Asset and Data Lifecycle Mapping Register.
- Facilitate secure information sharing when appropriate through:
  The use of information sharing protocols when sharing information with partner organisations.
  The use of disclosure and non-disclosure agreements when contractual arrangements give employees of other organisations access to our information.
- Provide management information from their directorate to enable the Leadership Team and other key stakeholders to have an effective overview of compliance with information-related legislation and regulations.

Knowledge, Skills and Experience

- Good understanding of the work of own function, including broadly who does what and the information held.
- Sound knowledge of policy, supporting standards and procedures, including procedures for handling requests for information, impact assessments and monitoring employees.
- Up-to-date broad knowledge of information-related legislation, regulations and professional standards that impact on the delivery of function's services.
- Competent user of IT with a broad understanding of the risks and issues associated with its use.
- Good interpersonal and communication skills (written and verbal).
- Good negotiating and facilitation skills, including ability to work with all levels of employees (including senior management).
- Able to demonstrate sensitivity and handle conflict.
- Proven ability to multi-task and manage a diverse portfolio of activities.

Appendix 4: Personal Data Breach Procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the 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 DPO will alert the Principal, CEO and Chair of Trustees.
- The 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.
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data.
  - Discrimination.
  - Identify theft or fraud.
  - Financial loss.
  - Unauthorised reversal of pseudonymisation (for example, key-coding).
  - Damage to reputation.
  - Loss of confidentiality.
  - Any other significant economic or social disadvantage to the individual(s) concerned.

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

- The 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.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach.
  - The categories and approximate number of individuals concerned.
  - The categories and approximate number of personal data records concerned.
  - The name and contact details of the DPO.
  - A description of the likely consequences of the personal data breach.
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The 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 DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO.
  - A description of the likely consequences of the personal data breach.
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

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

Appendix 5: Privacy Notice (Pupils)

This letter might be difficult for you to understand. You can ask your parents or another adult such as your teacher to This letter might be difficult for you to understand. You can ask your parents or another adult, such as your teacher, to help you understand it.

It is about how we use information about you and what we do with it. We call this information about you 'personal data' or 'personal information.'

Who we are

Your school is called **The X Academy** and this is part of the **Eastwood Park Academy Trust (EPAT).** EPAT is the organisation which is in charge of your personal information. This means that EPAT is the Data Controller.

The postal address of EPAT is: **The Eastwood Academy, Rayleigh Road, Leigh-on-Sea, Essex, SS9 5UU.**

If you want to contact us about your personal information, you can contact our Data Protection Officer (DPO) who is **Lauri Almond** and is contactable via igs@essex.gov.uk and 03330 322970. You can also leave a letter at Reception or send one by post.

The categories of pupil information that we process

- Personal identifiers and contacts (such as name, unique pupil number, contact details and address).
- Characteristics (such as ethnicity, language, and free school meal eligibility).
- Safeguarding information (such as court orders and professional involvement).
- Special educational needs (including the needs and ranking).
- Medical and administration (such as GP information, child health, dental health, allergies, medication and dietary requirements).
- Attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended).
- Assessment (attainment and progress).
- Behavioural information (such as exclusions and any relevant alternative provision put in place).
- Information about free school meal and pupil premium eligibility.
- Information for catering management purposes (e.g. whether you have school meals and how often).
- Information about biometric recognition systems (such a cashless catering).
- Anything related to school trips.

How we use pupil information

EPAT 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 your learning.
- Monitor and report on your progress.
- Provide appropriate care for you.
- Assess the quality of our services.
- To keep children safe (food allergies or emergency contact details).
- To comply with the statutory duties placed on us by the DfE data collections.

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. The use of your information for these purposes is lawful for the following reasons:

- EPAT is under a legal obligation to collect the information or the information is necessary for us to meet legal requirements imposed upon us such as our duty to safeguard pupils.
- It is necessary for us to hold and use your information for the purposes of our functions in providing schooling and so we can look after our pupils. This is a function which is in the public interest because everybody needs to have an education. This means we have a real and proper reasons to use your information.
- We will not usually need your consent to use your information. However, if at any time it appears to us that we would like to use your personal data in a way which means that we would need your consent, then we will explain to you what we want to do and ask you for consent. This is most likely to be where we are involved in activities which are not really part of our job as a Trust but we are involved because we think it would benefit our pupils. If you give your consent, you may change your mind at any time. If we think that you will not understand what we are asking then we will ask your parent or carer instead. Usually, we will involve your parents even if you can make your own decision.

How we collect pupil information

When we collect personal information on our forms, we will make it clear whether there is a legal requirement for you or your parents to provide it, whether there is a legal requirement on the Trust to collect it. If there is no legal requirement, then we will explain why we need it and what the consequences are if it is not provided.

We will also obtain information from your previous school, usually via secure file transfer from your previous school.

When we give your information to others

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 DPO. This right is transferred to the child once they reach the age 16. For more information about services for young people, please go to our local authority website 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 you that we hold, please contact the DPO.

We are required, by law (under regulation 5 of the Education (Information about Individual Pupils) England Regulations 2013, to pass some information about our pupils to the Department for Education (DfE). This is the part of the Government which is responsible for schools. This information may, in turn, then be made available for use by Southend Local Authority.

The DfE may also share information about pupils that we give to them, with other people or organisations. This will only take place where the law, including the law about data protection allows it.

The National Pupil Database (NPD) is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the DfE, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to national pupil database: user guide and supporting information - GOV.UK.

The DfE may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- Conducting research or analysis.
- Producing statistics.
- Providing information, advice or guidance.

The DfE has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether the DfE releases data to third parties are subject to a strict approval process and 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.
- The arrangements in place to store and handle the data.

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the DfE's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact the DfE: https://www.gov.uk/contact-dfe

We will also normally give information about you to your parents or your main carer. Where appropriate, we will listen to your views first. We will also take family circumstances into account, in particular where a Court has decided what information a parent is allowed to have.

We will also disclose your personal data to:

- Your new school if you move schools.
- Disclosures connected with SEN support.
- School Nurse.
- School Counsellor.
- CAMHS (Child and Adolescent Mental Health Service).

The information disclosed to these people / services will include sensitive personal information about you. Usually this means information about your health and any special educational needs or disabilities which you have. We do this because these people need the information so that they can support you.

Our disclosure of your personal data is lawful for the following reasons:

- EPAT is under a legal obligation to disclose the information or disclosing the information is necessary for us to meet legal requirements imposed upon us such as our duty to look after our pupils and protect them from harm.
- It is necessary for us to disclose your information for the purposes of our functions in providing schooling. This is a function which is in the public interest.
- There is a substantial public interest in disclosing your information because it is necessary to keep our pupils safe from harm.
- We may not usually need consent to disclose your information. However, if at any time it appears to us that we would need consent then we ask before a disclosure is made.

It is in your vital interests for your personal information to be passed to these people or services. If we need consent to pass on your information we will ask you for consent once we think that you can understand what we are asking. This is because the law requires us to ask you if you can understand. Normally, we involve your parents too. By law, we won't need their consent if you can give it, but parents like to be involved because it is part of looking after you. Before you are old enough to understand we will ask your parents to consent for you.

We do not normally transfer your information to a different country which is outside the European Economic Area. This would only happen if one of your parents lives abroad or if you move to a new school abroad. If this happens we will be very careful to make sure that it is safe to transfer your information. We will look at whether that other country has good data protection laws for example. If we cannot be sure that it is safe then we will talk to you and your parents about it and make sure that you are happy for us to send your information. As this is not something we normally do and we don't know which country we might need to send your information to, we cannot tell you more about it now but if we want to transfer your data to a different country then we will tell you whether or not we think it is safe and why we have decided that.

How long we keep your information

We only keep your information for as long as we need to or for as long as the law requires us to. Most of the information we have about you will be in our pupil file. We usually keep these until your 25th birthday, unless you move to another school, in which case we send your file to your new school. We have a Records Retention Policy which can be accessed via EPAT's website - http://www.epat.education/index.php/policies-and-statements/other

Your rights

- You can ask us for a copy of the information we have about you.
- You can ask us to correct any information we have about you if you think it is wrong.
- You can ask us to erase information about you (although we may have good reasons why we cannot do this).
- You can ask us to limit what we are doing with your information.
- You can object to what we are doing with your information.
- You can ask us to transfer your information to another organisation in a format that makes it easy for them to use.

Further information

There is more information in the Trust's Data Protection Policy which can be accessed via EPAT's website http://www.epat.education/index.php/policies-and-statements/other

You can complain about what we do with your personal information. If you are not happy with our answer to your complaint. The Complaints Policy can be accessed via EPAT's website http://www.epat.education/index.php/policies-and-statements/other

If you remain unhappy with our answer to your complaint, then you can complain to the Information Commissioner's Office:

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

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.

Appendix 6: Privacy Notice (Staff)

Who we are

The X Academy is part of Eastwood Park Academy Trust (EPAT). For the purposes of Data Protection legislation, EPAT is the Data Controller. This means it is in charge of personal data about you.

The postal address of EPAT is: **The Eastwood Academy, Rayleigh Road, Leigh-on-Sea, Essex, SS9 5UU.**

If you want to contact us about your personal information you can contact our Data Protection Officer (DPO) who is **Lauri Almond** and is contactable via igs@essex.gov.uk and 03330 322970.

The categories of school information that we process

- Personal information (such as name, address, employee or teacher number, national insurance number).
- Characteristics information (such as gender, age, ethnic group).
- Contract information (such as start date, hours worked, post, roles and salary information).
- Work absence information (such as number of absences and reasons).
- Qualifications (and, where relevant, subjects taught).
- Payroll information (including bank account details).
- Sensitive information e.g. medical information, ethnic group and trade union membership if you supply it.
- Information about biometric recognition systems such a cashless catering.

How we use your information

We process personal data relating to those we employ to work at, or otherwise engage to work at, within EPAT. This is for employment purposes to assist in the running of the Trust and to enable individuals to be paid.

Collecting and using your information in this way is lawful because:

- The processing is necessary for the performance of your employment contract and, in the case of special category personal data, processing that personal data is necessary for performing or exercising obligations or rights which are conferred on us or on you by law in connection with your employment.
- The processing is necessary for the performance of a legal obligation to which EPAT is subject, for example our legal duty to safeguard pupils.
- In the case of special category personal data, the processing is necessary for a safeguarding purpose i.e. to protect pupils from harm. This is in the substantial public interest.
- The processing is necessary for the performance of our education function which is a function in the public interest.

How we collect workforce information

When we collect personal information on our forms, we will make it clear whether there is a legal requirement for you to provide it, and whether there is a legal requirement on the Trust to collect it. If there is no legal requirement then we will explain why we need it and what the consequences are if it is not provided.

We also collect information from a previous employer or educational establishment. You will know about this because you will have supplied us with the relevant contact details.

How we share your information with third parties

We will not share information about you with third parties without your consent unless the law allows us to.

We are required, by law, to pass on some of the personal data which we collect to:

- The local authority (Southend).
- The Department for Education (DfE).

Local Authority

We are required to share information about our workforce members with our local authority (Southend) under section 5 of the Education (Supply of Information about the School Workforce)(No 2) (England) Regulations 2007 and amendments.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children and young people with the DfE for the purpose of those data collections.

We are required to share information about our school employees with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

We disclose personal data about you to the Disclosure and Barring Service for the purposes of carrying out checks on your suitability for work with children.

We disclose details about you including national insurance number and absence information to our payroll provider to enable you to be paid.

We disclose details about you to our HR provider for the purposes of HR management.

We share your identity and pay information with HMRC in conjunction with your legal obligation to pay income tax and make national insurance contributions.
Where you have decided to become part of a salary sacrifice scheme such as that for child care vouchers, we share your details with the provider to the extent necessary for them to provide the vouchers to you.

We share your details with your pension provider in order to make sure that you pay the correct amount and maintain your entitlement to a pension upon your retirement. For teachers the scheme is the TPS, for support staff the scheme is LGPS

Our disclosures to third parties are lawful because one of the following reasons applies:

- The disclosure is necessary for the performance of your employment contract.
- The disclosure is necessary for the performance of a legal obligation to which EPAT is subject.
- The disclosure is necessary for the performance of our education function which is a function in the public interest.
- We collect your consent.

For Special Category Personal Data uses:

- The disclosure is necessary for safeguarding purposes, i.e. to protect pupils from harm and is therefore in the substantial public interest.
- The disclosure is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on us as the Data Controller or on you in connection with your employment
- Where we collect ethnic origin or disability information for equality monitoring purposes, this falls within substantial public interest and is therefore lawful (but you are not required to provide information for that purpose if you do not want to)
- We collect your explicit consent.

How long we keep your personal information

We only keep your information for as long as we need it or for as long as we are required by law to keep it. Full details are given in our Records Retention Policy which can be accessed via EPAT's website http://www.epat.education/index.php/policies-and-statements/other

Your rights

- You can ask for access to your personal information.
- You can ask for rectification of the information we hold about you.
- You can ask for the erasure of information about you.
- You can ask for our processing of your personal information to be restricted.
- You can ask for data portability.
- You can object to us processing your information.

If you want to use your rights, for example, by requesting a copy of the information which we hold about you, please contact the Principal at the academy.

Further information

There is more information in the Trust's Data Protection Policy which can be accessed via the website http://www.epat.education/index.php/policies-and-statements/other

You can complain about what we do with your personal information. Refer to the Trust's Complaint's Policy which can be accessed via the website http://www.epat.education/index.php/policies-and-statements/other

If you remain dissatisfied with our answer to your complaint, then you can complain to the Information Commissioner's Office:

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

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.

Appendix 7: Consent to the Use of Personal Data Form

EPAT

Believe Succeed Together

Consent to the Use of Personal Data (Pupils)

The Trust requires your explicit consent with regards to the use of limited personal data.

Please indicate (✓) whether you consent or do not consent.

	I give consent	I do not give consent
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 unnamed photographs and videos of pupils in school e.g. fixed and electronic noticeboards, and out of school e.g. brochures, newsletters and Trust websites.		
Make use of named photographs and videos of pupils in school e.g. fixed and electronic noticeboards, and out of school e.g. brochures, newsletters and Trust 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.		
Obtain and use information pertaining to your child's fingerprint for the purpose of purchasing food and drink in the canteen.		

I understand that I can withdraw my consent at any stage.

Name of Pupil _____

Name of Parent: _____

Signature: _____

Date: _____

Appendix 8: Biometric Letter and Consent Form

EPAT

Believe Succeed Together

Biometric Information

Dear Parent,

The Trust would like to use biometric information pertaining to your child as part of an automated recognition system. Under the Protection of Freedoms Act 2012 (sections 26 to 28) the Trust must notify parents and obtain written consent before being able to use a child's biometric information.

'Biometric information' relates to a person's physical or behavioural characteristics that can be used to identify them. The Trust would like to use information from your child's fingerprint to allow them to purchase food and drink from the canteen. Specifically, the system will take measurements of your child's fingerprint and convert these measurements into a 'template' which is stored on the system.

In order to be able to use your child's biometric information, the written consent of at least one parent is required, although this will be overridden if the other parent objects. Similarly, if your child objects (in writing) the Trust cannot collect or use their biometric information. In both cases, written consent can be granted or withdrawn at any stage.

If you do not wish your child's biometric information to be processed by the Trust, or your child objects to such processing, the Trust will make alternative arrangements for your child to purchase food and drink from the canteen.

Please note that when your child leaves the Trust, or if for some other reason they cease using the biometric system, their biometric data will be securely deleted.

Yours sincerely,

Mr. N. Houchen
CEO

EPAT

Believe Succeed Together

Biometric Consent Form

Please complete this form indicating whether you do or do not consent to the Trust taking and using information pertaining to your child's fingerprint for the purpose of purchasing food and drink in the Canteen. By consenting, you are authorising the Trust to use your child's biometric information for this purpose until they leave the Trust or cease to use the system. If you wish to withdraw your consent at any time, this must be done, in writing, and sent to the constituent academy.

Once your child ceases to use the biometric recognition system, their biometric information will be securely deleted by the Trust.

Having read the guidance provided by the Trust, please indicate by ticking **one** of the boxes below whether or not you give consent to information from the fingerprint of your child being taken and used for the purpose of acquiring food and drink in the Canteen.

☐ I give consent

☐ I do not give consent

I understand that I can withdraw my consent at any stage.

Name of Pupil _____

Name of Parent: _____

Signature: _____

Date: _____