DATA PROTECTION/GENERAL DATA PROTECTION POLICY

Status	:	Statutory
Next revision due	:	June 2020
Reviewed and monitored by	:	DPO
Approved by	:	Local Governing Body
Signed by Chair of Local Governing Body	:	

Supporting documents:

Document Retention and Disposal Policy
Records Management Policy
Information Asset Register

Data Protection Policy for Shoeburyness High School

Background

The Data Protection Act (DPA) 1998 is the law that protects personal privacy and upholds individual's rights.

The EU General Data Protection Regulation 2016 (GDPR) comes into force on 25 May 2018 and replaces the Data Protection Act 1998. The changes introduced by the GDPR amount to the biggest reform of data protection and privacy law in over two decades. Some of the precise detail as to how the GDPR will be implemented here in the UK has yet to be decided. So, whilst this policy is a useful starting point, the school should continue to check the Information Commissioner's Office (ICO) website for further guidance.

The DPA/GDPR applies to anyone who handles or has access to people's personal data. **Shoeburyness High School** collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions.

The school must also let you know how we use your information and this is done through a Privacy Notice issued to pupils and parents. This summarises the information held on pupils, to include why it is held, the third parties to whom it may be passed on to and destruction timelines.

Scope

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. This includes names, addresses, telephone numbers and any expression of opinion about an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The school collects a large amount of personal data including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the school. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the DPA/GDPR, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

Compliance with the DPA/GDPR is the responsibility of all members of the school. Any deliberate breach of the DPA or this policy may lead to disciplinary action being taken, or even to a criminal prosecution.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;

3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security; Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

GDPR

From 25 May 2018, the school will need to be able to demonstrate that it complies with the following principles, which require that personal data is:

- processed in a lawful, fair and transparent manner
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate, and where necessary, kept up to date
- kept in a form which enables individuals to be identified for no longer than necessary
- processed in a manner that ensures appropriate security

Although the data protection principles are broadly the same, a new concept of “accountability" has been introduced which covers record keeping and being able to demonstrate compliance.

The rights of individuals

The school is already familiar with the right of subject access. This right is changing slightly under the GDPR and more is detailed in Appendix 1.

The GDPR also grants individuals additional rights, which include the following:

- right to be forgotten
- right to data portability

Definitions

Personal data

Like the DPA the GDPR applies to ‘personal data’. However, the GDPR’s definition is more detailed and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data.

For the school records with personal information, to include HR records, customer lists, or contact details, the change to the definition should make little practical difference. It can be assumed that if a school holds information that falls within the scope of the DPA, it will also fall within the scope of the GDPR.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

Sensitive personal data

The GDPR refers to sensitive personal data as “special categories of personal data”. These categories are broadly the same as those in the DPA, and is personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation but there are now some minor changes.

For example, the special categories data now specifically includes ‘genetic data’ and ‘biometric data’ where processed to ‘uniquely identify an individual’.

(Data relating to criminal offences and convictions are now addressed separately.)

Data Protection Officers - DPO

Under the GDPR, *'any public body or authority'* is required to appoint a DPO, but there is no clear-cut guidance as to which institutions qualify as such. Until further guidance is published on this point, all academies (and schools which are already subject to Freedom of Information Act legislation) should assume they will be required to appoint a DPO.

Whilst many schools have already appointed a 'data protection compliance manager' or similar, under GDPR, the DPO receives protected employment status and must:

- be suitably qualified, and an expert in data protection law
- be able to carry out the role independently
- report to the highest level of management

The DPO can either be engaged as an employee or a sub-contractor, and one DPO can act as the DPO for a number of public bodies.

Use of Personal Information by the School

The school will, from time to time, make use of personal information relating to pupils, their parents or guardians in the following ways:

- Could use photographic images of pupils in school publications and on the school website.
- For fundraising, marketing or promotional purposes and to maintain relationships with pupils of the school, including transferring information to any association society or club set up for the purpose of establishing or maintaining contact with pupils.

Consent

Signed consent to take photographs or record images of children will be requested from the parent or carer on enrolment of their child. The purpose for taking any images is to be clearly explained and agreed. Any consent given is to be reviewed on a regular basis (of a period of no more than one year) until such time the child or young person will no longer attend the school.

Obtaining an individual's consent to process personal/sensitive personal data or to transfer personal data outside the EU must now be explicit and will become much harder under GDPR. Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and you will need to provide simple ways for people to withdraw consent.

Children

The GDPR identifies children as "vulnerable individuals" deserving of "special protection". To that end, the School needs to be aware that the new rules introduce some child-specific provisions, most notably in the context of legal notices and the legal grounds for processing children's data.

When dealing with children (i.e. those under 13 years), consent from a child regarding online services will have to be authorised by a parent. Children's "right to be forgotten" will also become stronger.

The school therefore has reviewed how it seeks, records and manages consent and implemented appropriate mechanisms in order to ensure an effective audit trail.

Additionally, systems and procedures have been reviewed to ensure mechanisms are in place to deliver the rights of data subjects under the GDPR, including the right to be forgotten.

Data Protection by Design and Data Protection Impact Assessments

The school has to implement appropriate technical and organisational measures to show that it integrates data protection into its processing activities. It also understands and has put processes in place to conduct Data Protection Impact Assessments to assess the risks on projects/activities that process personal data.

Staff Training

All staff who have access to personal data have received training in DPA/GDPR following the changes coming into place. The school has also ensured that it keeps records of who has received training and when.

Personal Data Breaches

The school has revisited its internal procedures for detecting, reporting and investigating personal data breaches (as detailed in Appendix 2). GDPR requires mandatory breach notification to the regulator and in some cases also to affected individuals. Non-compliance can lead to administrative fines of up to €10m and the more serious breaches can lead to fines of up to €20m.

International Data Transfers

Under current data protection law, transfers of personal data outside the European Economic Area (EEA) are restricted and this will continue to be the case under GDPR.

The School has reviewed and mapped any flows of personal data outside the EEA, and considered what transfer mechanisms are in place and whether these comply with GDPR or not. This will apply if the School sends personal data outsider the EEA through the use of service providers such as Cloud Service Providers, bulk emailing services, web hosting services or simply communicating with parents or agents overseas.

Breach of the GDPR's rules on data transfers will be subject to maximum level fines of €20m.

General Statement

How, why and where we keep and use data about data subjects is coming under ever closer scrutiny.

The school is aware and has prepared for the changes as Ofsted are likely to continue its policy of heavily criticising schools and academies for data protection breaches.

The school is committed to maintaining the above principles at all times and will:

- inform data subjects, this could be pupils, parents or staff why they need their personal Information, how they will use it and with whom it may be shared through Privacy Notices (Appendices 3 & 4)
- check the quality and accuracy of the information held
- ensure that information is not retained for longer than is necessary
- when information is authorised for disposal it is securely destroyed
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- only share personal information with others when it is necessary and legally appropriate to do so
- set out clear procedures for responding to requests from data subjects, to include: access to personal information known as subject access requests, or the right to be forgotten
- train all staff so that they are aware of their personal responsibilities under data protection
- through robust contractual agreements, ensure that all contractors/third party providers, to include cloud providers are aware of their obligations to the school under data protection .

Data Retention Statement

Shoeburyness High School records are kept to:

- Meet current and future educational/business needs;
- Comply with statutory, legal and corporate governance best practice requirements;
- Ensure that the way we manage records is documented, understood and implemented; and
- Meet the reasonable current and future needs of internal and external stakeholders.

Records that are no longer required are eliminated as early as possible in an authorised and systematic manner. The benchmark for the retention of our records is 7 years except where stipulated otherwise in line with our Information Asset Register.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy and any queries should be directed to either the Head teacher or the DPO, (Dr Fran Haddock)

Complaints relating to information handling may be referred to the Information Commissioner's Office.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 03031231113.

Review

This policy will be reviewed as it is deemed appropriate, but at least every 2 years.
The policy review will be undertaken by the Head teacher, or nominated representative.

Appendix 1

Procedures for responding to subject access requests made under the DPA/GDPR. Under the DPA/GDPR any individual has the right to make a request to access the personal information held about them.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email**.** If the initial request does not clearly identify the information required, then further enquiries will be made. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

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

This list is not exhaustive.

2. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 13 or above) and the nature of the request. The Head teacher/DPO should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

3. A charge can no longer be made for responding to a subject access request (unless particular circumstances apply) and the time for responding to a subject access request is being reduced from 40 days to one month.

4. The DPA/GDPR have exemptions/derogations as to the provision of some information; therefore all information needs to be reviewed prior to disclosure.

5. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained.

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

7. If there are concerns over the disclosure of information then additional advice should be sought.

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

9. Information disclosed should be clear and legible and should have no codes or technical jargon.

10. The data subject should be consulted when taking into account the mode of delivery. If postal systems have to be used then registered/recorded mail must be used.

Appendix 2

Data Protection - Data Breach Procedure for Shoeburyness High School
The GDPR will apply in the UK as of 25 May 2018

Policy Statement

Shoeburyness High School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

This procedure applies to all personal and sensitive data held by Shoeburyness High School and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Shoeburyness High School if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations (GDPR)
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the DPO (Dr F Haddock), shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO in accordance with Article 55. This is UNLESS the personal data breach is unlikely to result in a risk to the rights and freedoms of persons.
2. The processor shall notify the DPO (Dr F Haddock) without undue delay after becoming aware of a personal data breach.
3. The notification provided by the DPO will:
   (a) Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned
   (b) Communicate the name and contact details of the data protection officer or other contact point for more information
   (c) Describe the likely consequences of the personal data breach
   (d) Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. The DPO shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Types of Breach

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a Data Breach

In the event that the School identifies or is notified of a personal data breach, the following steps should followed:

1. The person who discovers/receives a report of a breach must inform the Head Teacher or, in their absence, either the Deputy Head Teacher and/or the School's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
2. The DPO must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.
3. The Headteacher/DPO must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.
4. The Head Teacher/DPO must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the Essex Legal Services should be obtained.
5. The Head Teacher/DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

    a. Attempting to recover lost equipment.
    b. Contacting the relevant County Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned.
    c. Contacting the County Council's Communications Division if part of the crisis service, so that they can be prepared to handle any press enquiries.
    d. The use of back-ups to restore lost/damaged/stolen data.
    e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
    f. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Head Teacher/DPO to fully investigate the breach. The DPO should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Head Teacher/DPO should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish. The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the Head Teacher/DPO should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Leadership Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources (ZGO) for advice and guidance.

Implementation

The Head Teacher/DPO should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher.

Appendix 3 – Staff Privacy Notice

PRIVACY NOTICE – Data Protection Act 1998
School Workforce: those employed or otherwise engaged to work at a school or the Local Authority

SECAT are the Data Controller for the purposes of the Data Protection Act. As from May 2018 the General Data Protection Regulation (GDPR) rules will apply and we will follow this legislation, paying particular attention to both Article 6 'Lawfulness of processing' and Article 9 'Processing of special categories of personal data"' to collect personal information from you. We may receive information about you from your previous employer/school and the Learning Records Service.

The categories of workforce information that we collect, process, hold and share include:

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- relevant medical information and addresses

Why we collect and use this information

Personal data is held by academies within SECAT about those employed or otherwise engaged to work at one of the academies within SECAT. This is to assist in the smooth running of the Trust and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

- Improving the management of school workforce data across the sector;
- Enabling a comprehensive picture of the workforce and how it is deployed to be built up;
- Informing the development of recruitment and retention policies;
- Allowing better financial modelling and planning;
- Enable individuals to be paid
- Enabling ethnicity and disability monitoring; and
- Supporting the work of the School Teacher Review Body

The lawful basis on which we process this information

We process the information under the General Data Protection Regulation (GDPR); Article 6 'Lawfulness of processing' and Article 9 'Processing of special categories of personal data"' to collect personal information from you and we may receive information about you from your previous employer/school. For required data collection purposes for census information we also adhere to the Education Act 1996.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain workforce information to us or if you have a choice in this.

Storing this information

In line with the Retention Schedule, we will hold employee data for up to six years after the employee leaves the

relevant academy and any subsequent destruction of employee's personal data will be secure and logged appropriately by the relevant academy within SECAT.

Who we share this information with

We are required by law to routinely share some of this data with;

- Our local authority to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments. In addition, for payroll, absence, and employee relations purposes.

- The Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding; expenditure and the assessment educational attainments.

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

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The DfE may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal 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; and
- the arrangements in place to securely store and handle the data

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

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

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

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

Requesting access to your personal data
Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the relevant academy using the website below for contact information:

www.secat.co.uk

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

What decisions can you make about your information?
From May 2018 data protection legislation gives you a number of rights regarding your information. Some of these are new rights whilst others build on your existing rights. Your rights are as follows:

- if information is incorrect you can ask us to correct it
- you can also ask what information we hold about you and be provided with a copy. We will also give you extra information, such as why we use this information about you, where it came from and what types of people we have sent it to
- you can ask us to delete the information that we hold about you in certain circumstances. For example, where we no longer need the information
- you can ask us to send you, or another organisation, certain types of information about you in a format that can be read by computer
- our use of information about you may be restricted in some cases. For example, if you tell us that the information is inaccurate we can only use it for limited purposes while we check its accuracy

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:
If you need more information about how the LA and DfE store and use your information, then please go to the following websites:

www.southend.gov.uk

or

http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you cannot access these websites, please contact the LA or DfE as follows:

- Data Protection
  Department for People
  Southend-on-Sea Borough Council
  Civic Centre

Victoria Avenue
Southend
Essex. SS2 6ER
Contact number: 01702 215007
Email contact address: council@southend.gov.uk

- Ministerial and Public Communications Division
  Department for Education
  Piccadilly Gate
  Store Street
  Manchester
  M1 2WD
  Website: www.education.gov.uk
  Email: https://www.gov.uk/contact-dfe
  Telephone: 0370 000 2288

Appendix 4 – PUPIL Privacy Notice

Privacy Notice (How we use pupil information)

Why do we collect and use pupil information?

We, Shoeburyness High School, are a data controller for the purposes of the Data Protection Act 1998 and the Education Act of 1996. As from May 2018 the General Data Protection Regulation (GDPR) rules will apply and we will follow this legislation, paying particular attention to both Article 6 'Lawfulness of processing' and Article 9 'Processing of special categories of personal data"' to collect personal information from you and we may receive information about you from your previous school and the Learning Records Service.

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility, special educational needs)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- National curriculum assessment results
- Relevant medical information where applicable

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the GDPR, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

In line with the Retention Schedule we will hold pupil data for up to six years after they leave the school and any subsequent destruction of pupils personal data will be secure and logged appropriately.

Who do we share pupil information with?

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)

Aged 14+ qualifications

For pupils enrolling for post 14 qualifications, the Learning Records Service will give us a pupil's unique learner number (ULN) and may also give us details about the pupil's learning or qualifications

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:
To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services
What is different about pupils aged 13+?
Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent / guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

Our pupils aged 16+
We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit the local authority website.

The National Pupil Database (NPD)
The 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 department, 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 https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department 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 Department 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 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: and
- 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 department'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 DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, please contact the School Administrator.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means and profiling
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations
- data portability (this is a new enhancement to the right of subject access)

What decisions can you make about your information?
From May 2018 data protection legislation gives you a number of rights regarding your information. Some of these are new rights whilst others build on your existing rights. Your rights are as follows:

- if information is incorrect you can ask us to correct it

- you can also ask what information we hold about you and be provided with a copy. We will also give you extra information, such as why we use this information about you, where it came from and what types of people we have sent it to
- you can ask us to delete the information that we hold about you in certain circumstances. For example, where we no longer need the information
- you can ask us to send you, or another organisation, certain types of information about you in a format that can be read by computer
- our use of information about you may be restricted in some cases. For example, if you tell us that the information is inaccurate we can only use it for limited purposes while we check its accuracy

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:

If you need more information about how the LA and DfE store and use your information, then please go to the following websites:

www.southend.gov.uk or

http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you cannot access these websites, please contact the LA or DfE as follows:

- Data Protection
  Department for People
  Southend-on-Sea Borough Council
  Civic Centre
  Victoria Avenue
  Southend
  Essex. SS2 6ER
  Contact number: 01702 215007
  Email contact address: council@southend.gov.uk

- Ministerial and Public Communications Division
  Department for Education
  Piccadilly Gate
  Store Street
  Manchester
  M1 2WD
  Website: www.education.gov.uk
  Email: https://www.gov.uk/contact-dfe
  Telephone: 0370 000 2288

  You can also contact the school directly:
  Telephone 01702 292286
  Email: schooloffice@shoeburyness.southend.sch.uk