



Staplehurst School

# Data Protection, Records Management and Freedom of Information Policies

	<b>Date</b>
Policy reviewed and approved for Staff Consultation at a meeting of <b>The Full Governing Body</b>	21 May 2018
Policy to be next reviewed	<b>September 2018</b>

**Acting Data Protection Officer (DPO) is Mr. Callum Glazier email [DPO@staplehurst.kent.sch.uk](mailto:DPO@staplehurst.kent.sch.uk)**

These policies will be updated every two years or more frequently as necessary to reflect best practice or amendments made to the Data Protection & Freedom of Information legislation.

# Contents

<b>Part 1 - GDPR and Data Protection Policy</b>	<b>3</b>
Policy Objectives	3
Scope of the Policy	3
The Principles	3
Transfer Limitation	4
Lawful Basis for processing personal information	4
Sensitive Personal Information	5
Automated Decision Making	5
Data Protection Impact Assessments (DPIA)	6
Documentation and records	6
Privacy Notice	7
Purpose Limitation	7
Data minimisation	7
Individual Rights	7
Individual Responsibilities	8
Information Security	9
Storage and retention of personal information	9
Data breaches	10
Training	10
Consequences of a failure to comply	10
Review of Policy	10
The Supervisory Authority in the UK	10
<b>Part 2 - Records Management Policy</b>	<b>11</b>
Scope of the policy	11
Responsibilities	11
Relationship with existing policies	11
<b>Part 3 - Freedom of Information Policy and Publication Scheme</b>	<b>12</b>
Introduction	12
What is a publication scheme and why has it been developed?	12
Aims and objectives	12
Categories and classes of information published	12
Class 1, 2 & 3: School Information	12
Class 4: Governors' documents	13
Class 5: Our policies and procedures	14
Class 6 & 7: Lists and Registers and the services we offer	16
How to Request Information	16
Paying for Information	16
Responsibilities	16
Feedback and Complaints	16
<b>Appendix 1 – Glossary of Terms used in Part 1</b>	<b>17</b>
<b>Appendix 2 - Privacy Notices</b>	<b>19</b>
<b>Appendix 3 - Procedure for Access to Personal Information</b>	<b>26</b>
<b>Appendix 4 – Guidance for Staff on Security of Personal Information</b>	<b>28</b>
<b>Appendix 5 – Other Non-Statutory Documents held by the school</b>	<b>29</b>

# Part 1 - GDPR and Data Protection Policy

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

**See Appendix 1 for Glossary of Terms used in Part 1**

## Policy Objectives

The school as the Data Controller will comply with its obligations under the GDPR and DPA. The school is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the GDPR, therefore it is imperative that the School and all staff comply with the legislation.

## Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information<sup>1</sup>. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

The School collects a large amount of personal data every year including: pupil records, 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.

## The Principles

The principles set out in the GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**)
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**)
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**)

---

<sup>1</sup> GDPR Article 4 Definitions

6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

## Transfer Limitation

In addition, personal data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards<sup>2</sup>.

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the EEA.

## Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school
- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party<sup>3</sup>
- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent from be kept separate from those other matters

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first consented.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the school's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the school's public tasks) a legitimate interests assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

---

<sup>2</sup> These may be provided by a legally binding agreement between public authorities or bodies, standard data protection clauses provided by the ICO or certification under an approved mechanism.

<sup>3</sup> The GDPR states that legitimate interests do not apply to processing carried out by public authorities in the performance of their tasks, Article 6 However, the ICO indicates that where there are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate (particularly relevant for public authorities with commercial interests).

## Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited<sup>4</sup> unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on previous page
- One of the special conditions for processing sensitive personal information applies:
  - a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
  - b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
  - c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
  - d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
  - e) the processing relates to personal data which are manifestly made public by the data subject
  - f) the processing is necessary for the establishment, exercise or defence of legal claims
  - g) the processing is necessary for reasons of substantial public interest
  - h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
  - i) the processing is necessary for reasons of public interest in the area of public health.

The school's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the School can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the school can demonstrate compliance with the GDPR.

## Automated Decision Making

Where the school carries out automated decision making (including profiling) it must meet all the principles and have a lawful basis for the processing. Explicit consent will usually be required for automated decision making (unless it is authorised by law or it is necessary for the performance of or entering into a contract).

Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling. The School must as soon as reasonably possible notify the data subject in writing that a decision has been taken based on solely automated processing and that the data subject may

---

<sup>4</sup> GDPR, Article 9

request the school to reconsider or take a new decision. If such a request is received staff must contact the DPO as the school must reply within 21 days.

## **Data Protection Impact Assessments (DPIA)**

All data controllers are required to implement 'Privacy by Design' when processing personal data.

This means the School's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information.

Staff should adhere to the Data Protection Toolkit for Schools from the DfE with reference to the DPIA template.

When carrying out a DPIA, staff should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

## **Documentation and records**

Written records of processing activities must be kept and recorded including:

- the name(s) and details of individuals or roles that carry out the processing
- the purposes of the processing
- a description of the categories of individuals and categories of personal data
- categories of recipients of personal data
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures.

As part of the School's record of processing activities the DPO will document, or link to documentation on:

- information required for privacy notices
- records of consent
- controller-processor contracts
- the location of personal information;
- DPIAs and
- Records of data breaches.

Records of processing of sensitive information are kept on:

- The relevant purposes for which the processing takes place, including why it is necessary for that purpose
- The lawful basis for our processing and
- Whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

The School should conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- Carrying out information audits to find out what personal information is held
- Talking to staff about their processing activities
- Reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

## Privacy Notice

The school will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the data controller and the DPO, how and why the School will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data. The school must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

The School will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The School will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes. (See Appendix 2 for the School's Privacy Notices)

## Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

## Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The School maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

## Individual Rights

Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed (see Appendix 2 for the relevant privacy notice)
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request (see Appendix 3 - Procedure for Access to Personal Information)
- To have data corrected if it is inaccurate or incomplete
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the school no longer need the personal information, but you require the data to establish, exercise or defend a legal claim
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the school are verifying whether it is accurate), or where you have objected to the processing (and the school are considering whether the school's legitimate grounds override your interests)
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format
- To withdraw consent to processing at any time (if applicable)
- To request a copy of an agreement under which personal data is transferred outside of the EEA.
- To object to decisions based solely on automated processing, including profiling
- To be notified of a data breach which is likely to result in high risk to their rights and obligations
- To make a complaint to the ICO or a Court.

## Individual Responsibilities

During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The school expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not school staff to access personal information if you have specific authority to do so
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the school's policies).
- not remove personal information, or devices containing personal information (or which can be used to access it) from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes.

## Information Security

The school will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's acceptable usage policy. See Appendix 4 Guidance for Staff on Security of Personal Information

The school will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

**Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.

**Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.

**Availability** means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with the GDPR and DPA.

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the school
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

## Storage and retention of personal information

Personal data will be kept securely in accordance with the school's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Staff should adhere to the KCC Information Management Toolkit for Schools on KELSI with reference to the Record Retention Schedule, available at the following link:

[http://www.kelsi.org.uk/\\_data/assets/word\\_doc/0012/60213/InformationManagementToolkitforSchoolsv4-2.docx](http://www.kelsi.org.uk/_data/assets/word_doc/0012/60213/InformationManagementToolkitforSchoolsv4-2.docx)

Personal information that is no longer required will be deleted in accordance with the Schools Record Retention Schedule.

## Data breaches

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

The school must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their line manager/DPO/Head teacher immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the School's agreed breach reporting process.

## Training

The school will ensure that staff are adequately trained regarding their data protection responsibilities.

## Consequences of a failure to comply

The school takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or the school's DPO.

## Review of Policy

This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or DPA.

## The Supervisory Authority in the UK

Please follow this link to the ICO's website (<https://ico.org.uk/>) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

## Part 2 - Records Management Policy

The School recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. This document provides the policy framework through which this effective management can be achieved and audited. It covers scope, responsibilities and relationships with existing policies.

### Scope of the policy

- This policy applies to all records created, received or maintained by staff of the school in the course of carrying out its functions.
- Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.
- A small percentage of the school's records will be selected for permanent preservation as part of the institution's archives and for historical research.

### Responsibilities

- The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Headteacher.
- The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and timely.
- Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

### Relationship with existing policies

This policy has been drawn up within the context of: Data Protection policy and Freedom of Information Publication Scheme, with other legislation or regulations (including audit, equal opportunities and ethics) affecting the school.

# Part 3 - Freedom of Information Policy and Publication Scheme

## Introduction

Under the Freedom of Information Act 2000 and since 1 January 2005 there has been a legal right for any person to make a request to a school for access to information held by that school. Schools are under a duty to provide advice and assistance to anyone requesting information and must respond to the enquiry promptly.

This is Staplehurst School's Freedom of Information Policy and Publication Scheme.

## What is a publication scheme and why has it been developed?

One of the aims of the Freedom of Information Act 2000 is that public authorities, including schools, should be clear and proactive about the information they will make public. To do this we must produce a publication scheme, setting out:

- the classes of information which we publish or intend to publish;
- the manner in which the information will be published; and
- whether the information is available free of charge, or on payment.

The scheme covers information already published and information which is to be published in the future. All information in our publication scheme is available in paper form and some is available on our website for you to download. Some information which we hold may not be made public, such as personal information.

This publication scheme conforms to the model scheme for schools approved by the Information Commissioner.

## Aims and objectives

The school aims to:

- enable every child to fulfil their learning potential, with education that meets the needs of each child;
- help every child develop the skills, knowledge and personal qualities needed for life and work.

This publication scheme is a means of showing how we are pursuing these aims.

## Categories and classes of information published

The publication scheme guides you to information which we currently publish (or have recently published) or which we will publish in the future. This is split into categories of information known as 'classes'.

### Class 1, 2 & 3: School Information

This section sets out information about; who we are and what we do, what we spend and how we spend it and what our priorities are and how we are doing

<b>Who we are and what we do &amp; what our priorities are and how we are doing</b>	
<b>School Information</b>	<p>Under the School Information Regulations, maintained schools, are required to publish the following details online:</p> <p><u>Contact Us</u> The school's name, postal address and telephone number, plus a contact name to whom enquiries should be addressed</p> <p><u>Admissions</u> If the local authority decides your admissions, give information on where and how this information can be accessed on the local authority's website</p> <p><u>Ofsted report</u> Information on where to access the school's most recent Ofsted report</p> <p><u>SATS results</u> The school's most recent key stage 2 results as published by the Secretary of State. The school must publish the percentage of key stage 2 pupils who achieved:</p> <ul style="list-style-type: none"><li>• the expected standard or above in reading, writing and maths</li><li>• average progress in reading, writing and maths</li></ul>



	<ul style="list-style-type: none"> <li>• an average ‘scaled score’ in reading and maths</li> <li>• a high level of attainment in reading, writing and maths</li> </ul> <p><u>School's Performance table</u> Information on how to access the School Performance Tables on the DfE website</p> <p><u>Curriculum</u> For each academic year, the content of the curriculum followed for each subject and details as to how additional information relating to the curriculum may be obtained and in relation to key stage 1, the names of any phonics or reading schemes in operation</p> <p><u>Pupil Premium</u> The school must publish a strategy for the school’s use of the pupil premium. For the current academic year, the school must include:</p> <ol style="list-style-type: none"> <li>the school’s pupil premium grant allocation amount</li> <li>a summary of the main barriers to educational achievement faced by eligible pupils at the school</li> <li>how the school will spend the pupil premium to address those barriers and the reasons for that approach</li> <li>how the school will measure the impact of the pupil premium</li> <li>the date of the next review of the school’s pupil premium strategy</li> </ol> <p>For the previous academic year, the school must include:</p> <ul style="list-style-type: none"> <li>• how we spent the pupil premium allocation</li> <li>• the impact of the expenditure on eligible and other pupils</li> </ul> <p><u>PE funding report</u> The school must publish:</p> <ul style="list-style-type: none"> <li>• how much funding the school received</li> <li>• a full breakdown of how we’ve spent the funding or will spend the funding</li> <li>• the effect of the premium on pupils’ PE and sport participation and attainment</li> <li>• how you’ll make sure these improvements are sustainable</li> </ul> <p><u>SEND Policy</u> The report prepared by the school under section 317(5) (a) of EA 1996 (duties of governing bodies in relation to special educational needs)</p> <p><u>Charging Policy</u> The school’s charging and remissions policy</p> <p><u>Complaints Procedure</u> The school must publish details of the school’s complaints procedure</p> <p><u>Prospectus</u> A statement of the school’s ethos and values</p> <p><u>Governors’ information and duties</u> The school must publish information about the school’s governors, including details of each governor’s:</p> <ul style="list-style-type: none"> <li>• business interests</li> <li>• financial interests</li> <li>• governance roles in other schools</li> <li>• the structure and responsibilities of the governing body and committees</li> </ul>
<b>School Improvement</b>	School Improvement Plan including performance indicators. All documents (other than those which the Governing Body deem to be Confidential) are available for viewing at the school; however we reserve the right to make a charge should you require your own copy
<b>What we spend and how we spend it</b>	
<b>Financial Information</b>	Financial information relating to projected and actual income and expenditure, procurement, contracts and financial audit. All documents are available for viewing at the school; however we reserve the right to make a charge should you require your own copy

**Class 4: Governors’ documents**

This section sets out information about how we make decisions. All the documents listed are available for viewing at the school; however we reserve the right to make a charge should you require your own copy

Class 4	Description
<b>Instrument of</b>	A statutory document “made” by the Local Education Authority which records:



<b>Government</b>	<ul style="list-style-type: none"> <li>the name of the school</li> <li>the category of school</li> <li>the name of the governing body</li> <li>the manner in which the governing body is constituted</li> <li>the total number of governors</li> <li>the term of office of each category of governor if less than four years</li> <li>the name of any body entitled to appoint any category of governor</li> <li>details of any trust</li> <li>if the school has a religious character, a description of the ethos</li> <li>the date the instrument takes effect</li> </ul>
<b>Minutes</b>	Agreed minutes of meetings of the Governing Body and its committees (current and last full academic year)
<b>Other documents</b>	<p>All the documents listed are available for viewing at the school; however we reserve the right to make a charge should you require your own copy:</p> <ul style="list-style-type: none"> <li>Standing Orders and Committee Terms of Reference</li> <li>Governing Body Code of Practice</li> <li>Governing Body Statement and Action Plan</li> </ul>

### Class 5: Our policies and procedures

This section sets out information about our policies & procedures. All the documents listed are available for viewing at the school or on the school website; however we reserve the right to make a charge should you require your own copy.

<b>Class 5</b>	<b>Description</b>	<b>Website or Hard copy</b>
<b>Accessibility plan</b>	Statement of policy for the participation of disabled pupils in the school's curriculum, on improving the accessibility of the physical environment and improving delivery of information to disabled pupils when required	Website
<b>Safeguarding (Child Protection) Policy</b>	Statement of policy for safeguarding and promoting the welfare of pupils at the school	Website
<b>Equality Policy</b>	Statement of policy for promoting race, gender and disability equality	Website
<b>Designated Teachers</b>	Designated Safeguarding Lead incorporated into the Safeguarding Policy	Website
<b>Early Years Foundation Stage</b>	Statement on the provision of education for Early Years (Foundation Stage).	Website
<b>Home/school agreement</b>	Statement of the school's aims and values, the school's responsibilities, the parental responsibilities and the school's expectations of its pupils, for example - home learning arrangements	Website
<b>Behaviour and Discipline (including anti-bullying) Policy</b>	Statement of general principles on behaviour and discipline and of measures taken by the Headteacher to prevent bullying. Also includes Exclusions information.	Website
<b>Spiritual Moral Social and Cultural policy</b>	Statement of policy with regard to Spiritual Moral Social and Cultural development including PSHE, Sex & Relationships, Drug education; and RE and Collective Worship	Website
<b>Special Educational Needs &amp; Disability Policy</b>	Information about the school's policy on providing for pupils with special and additional education needs and disability	Website
<b>Supporting pupils with medical conditions policy</b>	Information about the arrangements that are in place to support pupils with medical conditions	Website
<b>Allegations of abuse against staff policy</b>	A policy on allegations of abuse against staff	Hard cop/email



<b>Attendance Policy</b>	A policy to actively promote 100% attendance for all of our pupils	Website
<b>Capability Policy</b>	Statement of procedure is to assist and support employees whose performance is causing concern to attain the standards required	Hard copy/email
<b>Charging Policy</b>	A statement of the school's policy with respect to charges and remissions for any optional extra or board and lodging for which charges are permitted. e.g. school publications, music tuition, trips	Website
<b>Complaints Procedure</b>	Statement of procedures for dealing with complaints, which is included in the Prospectus	Website
<b>Confidentiality Policy</b>	Statement regarding the confidentiality of information held by the school	Website
<b>Curriculum Circulars and Statutory Instruments</b>	Any statutory instruments, departmental circulars and administrative memoranda sent by the Department for Education and Skills to the Headteacher or Governing Body relating to the curriculum	Hard copy/email
<b>E-Safety Policy</b>	A policy to promote the safe use of the internet in an educational environment	Website
<b>Finance Policy</b>	A policy detailing the commitment to providing sound financial controls, to achieving value for money and to being worthy custodians of public money.	Hard copy/email
<b>Fire Evacuation Procedure</b>	Evacuation procedure	Hard copy/email
<b>Governors' Allowance Policy</b>	Scheme for paying Governors expenses	Hard copy/email
<b>Governors Business Interests</b>	Record of Governors Business Interests	Website
<b>Health and Safety Policy and Risk Assessments Information</b>	Statement of general policy with respect to health and safety at work of employees (and others) and the organisation and arrangements for carrying out the policy	Hard copy/email
<b>Appraisal (Performance Management) Policy</b>	Statement of procedures adopted by the Governing Body relating to the performance management of staff and the annual report of the Headteacher of the effectiveness of appraisal procedures	Hard copy/email
<b>Planning, Assessment, Record Keeping and Reporting Policy</b>	A policy detailing planning, assessment, record keeping and reporting procedures.	Hard copy/email
<b>School session times and term dates</b>	Details of school session times and dates of school terms and holidays	Website
<b>Staff Absence</b>	Statement of procedure on managing staff absence	Hard copy/email
<b>Staff Discipline Conduct, Grievance and Harassment &amp; Bullying</b>	Statement of procedure for regulating conduct and discipline of school staff; and procedures by which staff may seek redress for grievance or harassment and bullying	Hard copy/email
<b>Staffing Structure Document</b>	An organisation chart of the staffing at the school.	Hard copy/email
<b>Pay Policy</b>	A policy to ensure fairness for all staff and to demonstrate that they are valued equally and receive proper recognition for their work	Hard copy/email
<b>Whistleblowing Policy</b>	A procedure to encourage employees to raise serious concerns, without fear of reprisal or victimisation	Hard copy/email
<b>Other documents</b>	Other Non Statutory Documents held by the school – see Appendix 5	



## Class 6 & 7: Lists and Registers and the services we offer

All the documents listed are available for viewing at the school or on the school website; however we reserve the right to make a charge should you require your own copy

Class 6	Description	Website or Hard copy
<b>Lists and Registers</b>	Any information the school is currently legally required to hold in publicly available registers <b>(THIS DOES NOT INCLUDE THE ATTENDANCE REGISTER)</b>	Hard copy/email
Class 7	Description	Website or Hard copy
<b>The services we offer</b>	Information about the services we offer, including leaflets, guidance and newsletters produced for the public and businesses	Website and Hard copy/email

## How to Request Information

If you require a paper version of any of the documents within the scheme, please contact the school by telephone, email, fax or letter. Contact details are set out below, or you can visit our website at [www.staplehurst.kent.sch.uk](http://www.staplehurst.kent.sch.uk).

Email: [office@staplehurst.kent.sch.uk](mailto:office@staplehurst.kent.sch.uk)  
 Tel: 01580 891765  
 Fax: 01580 891291

Contact address: Staplehurst School, Gybbon Rise, Staplehurst, Kent TN12 0LZ.

To help us process your request quickly, please clearly mark any correspondence '**PUBLICATION SCHEME REQUEST**' (in CAPITALS please).

If the information you are looking for isn't available via the scheme (and isn't on our website), you can still contact the school to ask if we have it.

## Paying for Information

Information published on our website is free. If you don't have Internet access, you can access our website using a local library or Internet cafe. If your request means that we have to do a lot of photocopying or printing, or pay a large postage charge, or is for a priced item such as some printed publications or videos, we will let you know the cost before fulfilling your request.

## Responsibilities

The Governing Body have discussed and agreed this Freedom of Information Policy and Publication Scheme. The Governing Body is responsible for the maintenance of this scheme. The Headteacher is responsible for the day-to-day provision of advice, guidance, publicity and interpretation of the school's policy.

## Feedback and Complaints

We welcome any comments or suggestions you may have about the scheme. If you want to make any comments about this publication scheme or if you require further assistance or wish to make a complaint, then initially this should be addressed to: Mrs C Farthing, Headteacher, Staplehurst School, Gybbon Rise, Staplehurst, Kent. TN12 0LZ.

If you are not satisfied with the assistance that you get, or if we have not been able to resolve your complaint and you feel that a formal complaint needs to be made then this should be addressed to the Information Commissioner's Office. This is the organisation that ensures compliance with the Freedom of Information Act 2000 and that deals with formal complaints. The address is: Information Commissioner's Office, First Contact Team, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF

Helpline: 0303 123 1113:  
 Website: [www.ico.gov.uk](http://www.ico.gov.uk)



## Appendix 1 – Glossary of Terms used in Part 1

**Automated Decision-Making (ADM):** when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

**Automated Processing:** any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. profiling is an example of automated processing.

**Consent:** agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

**Data Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. The school is the Data Controller of all personal data relating to its pupils, parents and staff.

**Data Subject:** a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

**Data Privacy Impact Assessment (DPIA):** tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

**Data Protection Officer (DPO):** the person required to be appointed in public authorities under the GDPR.

**EEA:** the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

**Explicit Consent:** consent which requires a very clear and specific statement (not just action).

**General Data Protection Regulation (GDPR):** General Data Protection Regulation ((EU) 2016/679). Personal data is subject to the legal safeguards specified in the GDPR.

**Personal data** is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

**Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**Privacy by Design:** implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

**Privacy Notices:** separate notices setting out information that may be provided to Data Subjects when the school collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, school workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

**Processing** means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

**Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

**Pseudonymisation or Pseudonymised:** replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.



**Sensitive Personal Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.

Under Consultation



## Appendix 2 - Privacy Notices

### A. PRIVACY NOTICE FOR STAPLEHURST SCHOOL PARENTS AND PUPILS

This notice explains what personal data (information) we hold about you (meaning you and/or your child for the purposes of this notice), how we collect, how we use and may share information about you. We are required to give you this information under data protection law.

#### Who are we?

Staplehurst School collects, uses and is responsible for certain personal information about you. When we do so we are regulated under the General Data Protection Regulation (GDPR) which applies across the European Union (including in the United Kingdom) and we are responsible as 'controller' of that personal information for the purposes of those laws. Our Acting Data Protection Officer is Mr. Callum Glazier.

#### The personal information we collect and use

In the course of providing education we collect the following personal information:

- Personal information (such as name, unique pupil number, contact details language, nationality, country of birth, and free school meal eligibility)
- Special category characteristics
  - Ethnicity
  - Special educational needs (SEN) information
  - Relevant medical information
- Attendance information (such as sessions attended, number of absences and absence reasons)
- National curriculum assessment results
- Personal information, special category information, assessment results and SEN information from schools that you previously attended
- Service support and involvement information from KCC teams working to improve outcomes for children and young people (such as SEND, Early Help, Free School Meals, Admissions)

#### How we use your personal information

We use your personal information to:

- Support pupil learning
- Monitor and report on pupil progress
- Moderate teacher assessment judgements
- Provide appropriate pastoral care and support services
- Assess the quality of our services
- Comply with the law regarding data sharing
- Support you to decide what to do after you leave our school
- Support or improve educational provision
- Ensure no children are missing education
- Support children at risk of permanent exclusion
- Support the primary, secondary and in-year admissions process
- Safeguard children and young people
- Improve the education and services we provide



### How long your personal data will be kept

We hold your education records securely until you change school. Your records will then be transferred to your new school, where they will be retained until you reach the age of 25, after which they are safely destroyed.

### Reasons we can collect and use your personal information

We collect and use pupil information under section 537A of the Education Act 1996, section 83 of the Children Act 1989, and to carry out tasks in the public interest. If we need to collect special category (sensitive) personal information, we rely upon reasons of substantial public interest (equality of opportunity or treatment).

If there is processing or sharing that relies on your consent, we will make this clear to you and ensure we seek your consent.

### Who we share your personal information with

- Department for Education (DfE) (statutory for school funding and educational attainment policy and monitoring) and other government agencies and local authorities as required (e.g. to resolve funding queries)
- Kent County Council teams working to improve outcomes for children and young people
- Commissioned providers of local authority services (such as education services)
- Schools or colleges that you attend after leaving us
- Local forums with schools and KCC representatives which support in-year fair access processes and support managed moves between schools
- Local multi-agency forums which provide SEND advice, support and guidance (such as Local Inclusion Forum Team (LIFT))
- Partner organisations signed up to the Kent & Medway Information Sharing Agreement, where necessary, which may include Police, school nurses, doctors and mental health workers and Kent Community Health NHS Foundation Trust
- Schools in our local collaboration, to enable the moderation of pupil assessment outcomes, to support collaborative working through joint analysis, and ensure children continue to receive appropriate education provision
- KCC has to share information with external moderators (teachers with recent relevant experience) of end of key stage assessments, to meet statutory requirements from the Standards & Testing Agency (STA)
- Third-party providers of information services where consent has been given
- Contracted providers of services (such as school photographers, SCOPay and catering providers) where consent has been given

We will share personal information with law enforcement or other authorities if required by applicable law. We are required to share information about our pupils with KCC and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

### The National Pupil Database (NPD)

The NPD is owned and managed by the DfE 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 DfE. 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.

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 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.

### Your Rights

Under the GDPR you have rights which you can exercise free of charge which allow you to:

- Know what we are doing with your information and why we are doing it (Privacy Notice)
- Ask to see what information we hold about you (Subject Access Request)
- Ask us to correct any mistakes in the information we hold about you
- Object to direct marketing
- Make a complaint to the Information Commissioners Office (ICO)
- Withdraw consent (if applicable)

Depending on our reason for using your information you may also be entitled to:

- Ask us to delete information we hold about you
- Have your information transferred electronically to yourself or to another organisation
- Object to decisions being made that significantly affect you
- Object to how we are using your information
- Stop us using your information in certain ways

We will always seek to comply with your request however we may be required to hold or use your information to comply with legal duties. Please note: your request may delay or prevent us delivering a service to you.

For further information about your rights, including the circumstances in which they apply, see the guidance from the UK ICO on individuals' rights under the GDPR.

If you would like to exercise a right, please contact [DPO@staplehurst.kent.sch.uk](mailto:DPO@staplehurst.kent.sch.uk).

### Keeping you personal information secure

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

### Who to Contact and Where to go for Further Information

Please contact [DPO@staplehurst.kent.sch.uk](mailto:DPO@staplehurst.kent.sch.uk) to exercise any of your rights, or if you have a complaint about why your information has been collected, how it has been used or how long we have kept it for.

If you would like to get a copy of the information about youth that KCC shares with the DfE or post-16 providers or how they use your information, please contact the Information Resilience and Transparency Team at [data.protection@kent.gov.uk](mailto:data.protection@kent.gov.uk).



For more information about services for children and young people, please go to:  
<http://www.kent.gov.uk/education-and-children> or the KCC website at [www.kent.gov.uk](http://www.kent.gov.uk)

The GDPR also gives you right to lodge a complaint with a supervisory authority. The supervisory authority in the UK is the Information Commissioner who may be contacted at <https://ico.org.uk/concerns> or telephone 03031 231113.

For further information visit <https://www.kent.gov.uk/about-the-council/about-the-website/privacy-statement>

For further information about how the Department for Education uses you information:

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 <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

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 DfE: <https://www.gov.uk/contact-dfe>

Under Consultation



## B. PRIVACY NOTICE FOR STAPLEHURST SCHOOL WORKFORCE

This notice explains what personal data (information) we hold about you, how we collect, how we use and may share information about you. We are required to give you this information under data protection law.

### Who are we?

Staplehurst School collects, uses and is responsible for certain personal information about you. When we do so we are regulated under the General Data Protection Regulation which applies across the European Union (including in the United Kingdom) and we are responsible as 'controller' of that personal information for the purposes of those laws. Our Acting Data Protection Officer is Mr. Callum Glazier.

The personal information we collect and use

- Information collected by us
- In the course of employing staff in our school we collect the following personal information when you provide it to us:
  - Personal information (such as name, address, contact details, employee or teacher number, national insurance number)
  - Characteristics (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

### How we use your personal information

We use your personal information to:

- Enable individuals to be paid
- Support pension payments and calculations
- Enable sickness monitoring
- Enable leave payments (such as sick pay and maternity leave)
- Develop a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- Inform financial audits of the school
- Fulfil our duty of care towards our staff
- Inform national workforce policy monitoring and development
- Enable the school to formulate emergency management & winter closure procedures

### How long your personal data will be kept?

We will hold your personal information for 6 years plus current in line with KCC's personnel retention record keeping guidelines. Except in respect of:

- Injuries at work when the information is retained for 12 years
- Ex-employees - termination plus 7 years
- Unsuccessful applicants - application are retained for 6 months

### Reasons we can collect and use your personal information

We rely on having a legitimate reason as your employer to collect and use your personal information, and to comply with our statutory obligations, and to carry out tasks in the public interest. If we need to collect special category (sensitive) personal information, we rely upon reasons of substantial public interest (equality of opportunity or treatment).

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

### Who we share your personal information with

- Department for Education (DfE)



- Kent County Council Management Information
- Kent County Council Schools Financial Services
- Our commissioned providers of personnel and payroll services - Medway Council
- Contracted providers of services (such as school photographer, SCOPay and catering providers) where consent has been given

We will share personal information with law enforcement or other authorities if required by applicable law.

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.

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 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 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 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.

### **Your Rights**

Under the GDPR you have rights which you can exercise free of charge which allow you to:

- Know what we are doing with your information and why we are doing it
- Ask to see what information we hold about you (Subject Access Requests)
- Ask us to correct any mistakes in the information we hold about you
- Object to direct marketing
- Make a complaint to the Information Commissioners Office
- Withdraw consent (if applicable)

Depending on our reason for using your information you may also be entitled to:

- Ask us to delete information we hold about you
- Have your information transferred electronically to yourself or to another organisation
- Object to decisions being made that significantly affect you
- Object to how we are using your information
- Stop us using your information in certain ways

We will always seek to comply with your request however we may be required to hold or use your information to comply with legal duties. Please note: your request may delay or prevent us delivering a service to you.

For further information about your rights, including the circumstances in which they apply, see the guidance from the UK Information Commissioners Office (ICO) on individuals' rights under the General Data Protection Regulation.



If you would like to exercise a right, please contact [DPO@staplehurst.kent.sch.uk](mailto:DPO@staplehurst.kent.sch.uk)

### **Keeping your personal information secure**

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

### **Who to Contact and Where to go for Further Information**

Please contact [DPO@staplehurst.kent.sch.uk](mailto:DPO@staplehurst.kent.sch.uk) to exercise any of your rights, or if you have a complaint about why your information has been collected, how it has been used or how long we have kept it for.

If you would like to get a copy of the information about you that KCC shares with the DfE or how they use your information, please contact the Information Resilience and Transparency Team at [data.protection@kent.gov.uk](mailto:data.protection@kent.gov.uk).

The General Data Protection Regulation also gives you right to lodge a complaint with a supervisory authority. The supervisory authority in the UK is the Information Commissioner who may be contacted at <https://ico.org.uk/concerns> or telephone 03031 231113.

For further information visit <https://www.kent.gov.uk/about-the-council/about-the-website/privacy-statement>

For further information about how the Department for Education uses your information:

To find out more about the staff information we share with the DfE, for the purpose of data collections, go to <https://www.gov.uk/education/school-workforce-censuses>

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 DfE: <https://www.gov.uk/contact-dfe>



## Appendix 3 - Procedure for Access to Personal Information<sup>5</sup>

### Rights of access to information

There are two distinct rights of access to information held by schools about pupils.

1. Under the GDPR an individual has a right to request access to their own personal information. In certain circumstances requests may be made by a parent on behalf of their child (see below).
2. The right of parents to have access to curricular and educational records relating to their child as defined within the Education (Pupil Information) (England) Regulations 2005.

These procedures relate to the above mentioned rights.

### Dealing with a request

1. Requests for personal information must be made in writing and addressed to the Headteacher. If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any personal 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.*

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand. As a general rule, a child of 12 or older is expected to be mature enough to understand the request they are making. If the child cannot understand the nature of the request, someone with parental responsibility can ask for the information on the child's behalf. The Headteacher should discuss the request with the child and take their views into account when making a decision.
4. The response time for subject access requests, once officially received, is one month (not working or school days but calendar days, irrespective of school holiday periods). In some circumstances this may be extended to a maximum of two further months. Requests for information from pupils or parents for access to information classed as being part of the education record must be responded to within 15 school days.
5. There are some exemptions to the right to subject access that apply in certain circumstances or to certain types of personal information. Therefore all information must be reviewed prior to disclosure.
6. Responding to a request may involve providing information relating to another individual (a third party). Third party information is that which identifies another pupil/parent or has been provided by another agency, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the statutory timescale.
7. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another individual involved should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.
8. If there are concerns over the disclosure of information then additional advice should be sought from KCC Information Resilience & Transparency Team (see contact details below).
9. Where redaction (information edited/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.

---

<sup>5</sup> To be replaced by KCC Model SAR when available interim the following GDPR adapted procedure shall apply



10. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.
11. Information can be viewed at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover.
12. The views of the applicant should be taken into account when considering the method of delivery. If the applicant has asked for the information to be posted then special next day delivery or recorded delivery postal service must be used.

### **Complaints**

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

### **Contacts**

If you have any queries or concerns regarding access to records or the Data Protection Act, then please contact:

Michelle Hunt  
The Information Resilience & Transparency Team  
Kent County Council  
Room 2.71, Sessions House,  
County Hall,  
Maidstone, Kent, ME14 1XQ  
Email: [michelle.hunt@kent.gov.uk](mailto:michelle.hunt@kent.gov.uk)  
Or [dataprotection@kent.gov.uk](mailto:dataprotection@kent.gov.uk)

Further advice and information can be obtained from the Information Commissioner's Office, [www.ico.gov.uk](http://www.ico.gov.uk)



## Appendix 4 – Guidance for Staff on Security of Personal Information

The Data Protection Act 1998 is a law that protects personal privacy and upholds an individual's rights. The seventh principle of the Act refers to appropriate security measures being taken to protect unauthorised or illegal processing.

All personal data whether manual or electronic must be kept secure to prevent accidental loss, damage or destruction. The extent of the security measures required will depend on the sensitivity of the data.

### Here are some basic Dos and Don'ts:

- Lock the office when leaving it unattended for any length of time to prevent unauthorised access to personal information.
- Manual records containing personal information should be locked away in a cabinet or drawer when not in use.
- When documents containing personal information have reached the end of their life dispose of them by shredding or use the confidential waste bins.
- Do not share your user ID or password with anyone.
- If you have a laptop which holds personal data, make sure it is encrypted.
- Ensure that your computer screen cannot be viewed by any unauthorised personnel.
- Do not send personal information by fax unless the information has been de-personalised or the fax machine is a 'safe haven' one (in a secure area, which is locked when unattended).
- Do not send personal information by unsecured email (outside of the kent.gov email system) as its security cannot be guaranteed. If it is necessary to send information in this way and you do not have access to secure email, make sure it has been either password protected or de-personalised. Send the data as an attachment to the email and flag as confidential.
- If you are required within the course of your duties to take personal data home (including laptops, videos, etc), do not leave the information unattended for any length of time, especially in a vehicle overnight.
- Do not give out personal information over the telephone; invite the caller to put the request in writing. If the request is urgent take the caller's name and switchboard telephone number and verify their details before responding.
- Do not discuss other people's personal business in public areas where conversations can be overheard by people with no right to know the details of the information.
- Remember - at all times treat people's personal information as you would wish your own to be treated.

Information Resilience & Transparency Team

Room 2.71

Sessions House

Email: [data.protection@kent.gov.uk](mailto:data.protection@kent.gov.uk)



## Appendix 5 – Other Non-Statutory Documents held by the school

All the documents listed are available for viewing at the school or on the school website; however we reserve the right to make a charge should you require your own copy.

<b>Name of document</b>	<b>Website or hard copy/email</b>
Art & Design Policy	Hard copy/email
Design Technology Policy	Hard copy/email
Educational Visits Policy	Hard copy/email
French Policy	Hard copy/email
Geography Policy	Hard copy/email
Academically More Able & Talented Policy	Website
History Policy	Hard copy/email
Homework Home Learning Policy	Website
ICT Policy	Hard copy/email
Literacy Policy	Website
Looked After Children Policy	Hard copy/email
Mathematics Policy	Website
Music Policy	Hard copy/email
Physical Activity Policy	Hard copy/email
School Food Policy	Website
Science Policy	Hard copy/email
School Travel Plan	Hard copy/email
School Visitors' Policy	Website
Spelling policy	Website