Data Protection Policy

	Signature	Date
Chair of Governors		
Headteacher		
Committee Approval		Spring 2020
Next Review Date		Spring 2022

Contents

1. Introduction and purpose

This policy sets out Newtown School's commitment to handling personal data in line with the EU General Data Protection Regulation 2016 and the UK Data Protection Act 2018 (collectively known as the data protection legislation).

Newtown School is the data controller for the personal data it processes and is registered with the Information Commissioner's Office (ICO) under registration Z7464712. Details about the registration can be found at www.ico.org.uk.

The purpose of this policy is to explain how Newtown School handles personal data under the data protection legislation, and to inform employees and other individuals who process personal information on behalf of the school's expectation in this regard.

2. Scope

This policy applies to the processing of personal data held by Newtown School. This includes personal data held about pupils, parents / carers, employees, temporary staff, governors, volunteers, visitors and any other identifiable data subjects.

This policy should be read alongside the school's Privacy Notice for Parents and Carers, Privacy Notice for the School Workforce and Privacy Notice for Governors and Volunteers, these are in the appendices.

3. Definitions

There are several terms used in the data protection legislation and in this policy, which must be understood by those who process personal data held by the school. These are:

Personal data: This is any information relating to an identified or identifiable living individual. This includes a name, identification number, location data, an online identifier, information relating to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Special categories of personal data: These are personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs and the trade union membership of the data subject.

Processing: This is any operation or set of operations which is performed on personal data, such as the collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data subject: This is an identifiable, living individual who is the subject of personal data.

Data Controller: This is an organisation who determines the purposes and means of processing of personal data.

Data Processor: This is an organisation or person who processes personal data on behalf of a data controller, on their instruction.

4. Roles and Responsibilities

4.1 Governors

The Board of Governors has overall responsibility for ensuring that the school implement this policy and continues to demonstrate compliance with the data protection legislation.

The policy will be reviewed at least every two years or when new procedures or legislation needs to be taken in to account.

4.2 Headteacher

The Headteacher has day to day responsibility for ensuring that this policy is adopted and adhered to by employees and other individuals processing personal data on the school's behalf.

4.3 Data Protection Officer

The Data Protection Officer is responsible for carrying out the tasks set out in Article 39 of the General Data Protection Regulation (GDPR). In Summary the DPO is responsible for:

- informing and advising the school of their obligations under data protection legislation
- monitoring compliance with data protection policies
- raising awareness and delivering training to employees
- carrying out audits on the school's processing activities
- providing advice regarding Data Protection Impact Assessments and monitoring performance
- co-operating with the Information Commissioner's Office
- acting as the contact point for data subjects exercising their rights

The DPO shall report directly to the Board of Governors and Senior Leadership Team and shall provide regular updates on the school's progress and compliance with the data protection legislation.

The DPO for Newtown School is: Simon Barker who can be contacted directly on simon.barker@newtown.education or via the school office.

4.4 Employees, temporary staff, contractors, volunteers and visitors

All employees, temporary staff, contractors, volunteers, visitors and other individuals processing personal data on behalf of the school are responsible for complying with the contents of this policy.

All individuals shall remain subject to the common law duty of confidentiality when their employment or relationship with the school ends. This does not affect an individual's rights in relation to whistleblowing.

Failure to comply with this policy may result in a disciplinary action or termination of employment or service contract.

5. Policy Content

5.1 Data Protection Principles

5.1.1 The GDPR provides a set of principles which govern how the school handle personal data. In summary, these principles state that personal data must be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary for the purpose it was processed
- accurate and where necessary kept up to date

- kept for no longer than is necessary
- processed in a manner that ensures appropriate security of the data

5.1.2 The school and all individuals processing personal data controlled by each school, shall comply with the data protection principles in the following manner:

5.2 Lawfulness, fairness and transparency

5.2.1 Lawful processing

Personal data will only be processed where there is a lawful basis for doing so. This will be where at least one of the following applies:

- The data subject has given consent
- It is necessary for the performance of a contract or entering into a contract with the data subject
- It is necessary for compliance with a legal obligation
- It is necessary to protect the vital interests of a person
- It is necessary for the performance of a task carried out in the public interest or in the exercise of official duties

5.2.2 When special categories of personal data are processed (for example, health or medical data, racial or ethnic origin or biometric data (e.g. facial images and fingerprints), this shall only be done where a lawful basis has been identified from the list above, and one from the following list:

- The data subject has given explicit consent
- The processing is necessary for the purposes of exercising or performing any right or obligation which is imposed on the school in relation to employment, social security and social protection law (e.g. safeguarding individuals at risk; protection against unlawful acts; prevention against fraud)
- It is necessary to protect the vital interests of any person where the data subject is physically or legally incapable of giving consent
- The processing is necessary for the establishment, exercise or defence of legal claims
- The processing is necessary in the substantial public interest
- The processing is necessary for the assessment of the working capacity of the employee

5.2.3 Consent

Most of the school's processing of personal data will not require consent from data subjects (or their parents/carers as appropriate), as the school need to process this data in order to carry out its official tasks and public duties as a school. However, there are circumstances when the school are required to obtain consent to process personal data, for example:

- To collect and use biometric information (such as fingerprints)
- To send direct marketing or fundraising information by email or text
- To take and use photographs, digital or video images and displaying, publishing or sharing these in a public arena such as:
  - on social media;
  - in the school' prospectus;
  - on the school' websites;
  - in the press/ media;
  - in the school' newsletters

When the school relies on consent as its lawful basis, it shall ensure the person providing it has positively opted-in to the proposed activity and is fully informed as to what they are consenting to and any non-obvious consequences of giving or refusing that consent. Consent shall not be assumed as being given if no response has been received e.g. a consent form has not been returned. Where consent is being obtained for the collection or use of children's information, consent shall be obtained from a parent or guardian.

The school shall ensure that where consent is obtained, there is a record of this. Where possible, consent shall be obtained in writing. All forms requesting consent shall include a statement informing the person of their right to withdraw, and an email address so they may notify the school of any changes or withdrawal of consent.

5.2.4 Fairness and transparency

The school shall be fair, open and transparent in the way it handles personal data, and will publish privacy notices which explain:

- What personal data the school process and why
- What our lawful basis is when we process that data
- Who we might share that data with
- If we intend to transfer the data abroad
- How long we keep the data for
- What rights data subjects have in relation to their data
- Who our Data Protection Officer is and how to contact them.

The school' privacy notices shall be clear, concise and easily accessible. Privacy notices will be provided to parents/carers of pupils when their child is enrolled at the school, which will explain how the school handles pupil information. This notice will be published on the school's website; parents will be directed to this on an annual basis. Employees will be given a privacy notice explaining how the school handles employee information when they join the school and directed to this annually thereafter. The school shall provide privacy notices to other categories of data subjects, as appropriate.

5.3 Purpose limitation

The school shall collect personal data for specified (i.e. as described in the school's privacy notices), explicit and legitimate purposes and shall not process this data in any way would could be considered incompatible with those purposes (e.g. using the data for a different and unexpected purpose).

5.4 Data minimisation

The school shall ensure the personal data it processes is adequate, relevant and limited to what is necessary for the purpose(s) it was collected for.

5.5 Accuracy of data

5.5.1 The school shall take all reasonable efforts to ensure the personal data it holds is accurate and where necessary kept up to date. Where personal data is found to be inaccurate, this information will be corrected or erased without delay.

5.5.2 The school will send frequent reminders, on at least an annual basis, to parents/carers, pupils and employees, to remind them to notify the school of any changes to their contact details or other information.

5.5.3 The school shall carry out sample checks of pupil and employee files containing personal data, to ensure the data is accurate and up to date. This will be carried out on an annual basis.

5.6 Storage limitation and disposal of data

5.6.1 The school shall keep personal data for no longer than is necessary for the purpose(s) of the processing. The school shall maintain and follow a Record Retention Schedule, which sets out the timeframes for retaining personal data. This schedule shall be published alongside the school' privacy notices on the website.

5.6.2 The school shall designate responsibility for record disposal/deletion to nominated employees, who shall adhere to the school's Record Retention Schedule and ensure the timely and secure disposal of the data.

5.7 Security of personal data

The school shall have appropriate security in place to protect personal data against unauthorised or accidental access, disclosure, loss, destruction or damage. This will be achieved by implementing appropriate technical and organisational security measures.

5.8 Technical security measures

The school shall implement proportionate security measures to protect its network and equipment and the data they contain. This includes, but is not limited to:

- having a Firewall, anti-virus and anti-malware software in place
- applying security patches promptly
- restricting access to systems on a 'need to know' basis
- enforcing strong password policies; passwords shall be a minimum of 8 characters in length; changed at appropriate intervals and not shared or used by others
- encrypting laptops, USB/memory sticks and other portable devices or removable media containing personal data
- regularly backing up data
- regularly testing the school' disaster recovery and business continuity plans, to ensure data can be restored in a timely manner in the event of an incident

5.9 Organisational security measures

The School will ensure the following additional measures are also in place to protect personal data:

- Employees shall sign confidentiality clauses as part of their employment contract
- Data protection awareness will be provided to employees during induction and annually thereafter
- Policies and guidance shall be in place relating to the handling of personal data whilst during and outside of school. These will be communicated to employees and other individuals as necessary, including policy revisions. A policy declaration shall be signed by employees and retained on their personnel file.
- Data protection compliance shall be a regular agenda item in Board of Governors and Senior Leadership Team meetings.
- Appropriate equipment and guidance will be available for employees to use and follow when carrying paperwork off school premises.
- The school's buildings, offices and where appropriate classrooms, shall be locked when not in use.
- Paper documents and files containing personal data shall be locked in cabinets/cupboards when not in use, and access restricted on a need to know basis.

Procedures shall be in place for visitors coming onto the premises. These will include signing in and out at reception and wearing a visitor's lanyard. and being escorted by a member of staff (unless the visitor holds a valid Disclosure and Barring Service certificate, or it is otherwise appropriate for the person not to be escorted).

Newtown School will have procedures in place to identify, report, record, investigate and manage personal data breaches in the event of a security incident.

5.10 Rights of Data subjects

5.10.1 Data subjects have several rights under data protection legislation. The school shall comply with all written requests from data subjects exercising their rights without delay, and within one month at the latest.

5.10.2 Data subjects have the right to:

- request access to the personal data the school holds about them and receive a copy of this information free of charge (the school reserves the right to charge for photocopying, postage and packaging);
- ask for the information the school holds about them to be rectified if it is inaccurate or incomplete;
- to ask in certain circumstances for the processing of their data to be restricted;
- object to the school processing their information for the 'performance of a task carried out in the public interest', except where the school can demonstrate compelling legitimate grounds;
- object to the school using their information for direct marketing purposes;
- stop the school processing their data if the school relied on consent as the lawful basis for processing, and they have subsequently withdrawn consent;
- complain to the school and the Information Commissioner's Office if they are not satisfied with how their personal data has been processed;
- request compensation from the school if they have suffered damage or distress as result of a breach of security involving their personal data.

5.11 Handling requests

5.11.1 Data subjects exercising their rights are recommended to put their request in writing and send it to the school as below. Data subjects can also exercise their rights verbally. In such cases each school will promptly write to the data subject outlining the verbal discussion / request and will ask the data subject to confirm this is accurate.

Simon Barker, DPO, Newtown School, Berkhampstead Road, Chesham, Bucks HP5 3AT

simon.barker@newtown.education or via the school office, 01494 783713

5.11.2 Data subjects who request a copy of their personal data (known as making a Subject Access Request) may be asked to provide identification to satisfy the school of their identity, particularly where the data subject is no longer a pupil, employee or governor at the school. These requests shall be responded to within 1 month, upon receipt of receiving a valid request and appropriate identification (where requested).

5.11.3 Pupil information requests

Pupils can request access to their own personal data when they have sufficient maturity to understand their rights; know what it means to make such a request and can interpret the information they receive. The Information Commissioner's Office and the Department for Education guidance, suggests that children aged 13 years and above, may have sufficient

maturity in these situations, however it is for each school to decide this on a case by case basis.

Parents/carers can make a request for their child's information when their child is 12 years and under

Where the child attends a maintained school, a parent can request a copy of their child's educational record. The parent/carer does not need consent from the child to access this information. This type of request is governed by the Education (Pupil Information) (England) Regulations 2005. These requests shall be responded to within 15 school days.

5.11.4 When responding to Subject Access Requests or pupil information requests, the school shall redact the information the data subject or parent/carer is not entitled to receive, in accordance with the exemptions set out in the Data Protection Act 2018.

5.11.5 The schools shall consult with the Data Protection Officer upon receipt of a Subject Access Request or pupil information request, and again prior to making disclosures in response to these requests.

5.12 Data protection by design and default

The school shall have appropriate technical and organisational measures in place which are designed to implement the data protection principles in an effective manner, and will ensure that by default, it will only process personal data where it is necessary to do so. The Newtown School Policy and supplementary policies, procedures and guides, explain how the school aims to achieve this.

5.13 Joint controller agreements

The school shall sign up to agreements with other data controllers where personal data is shared or otherwise processed on a regular basis, where it is necessary to do so.

5.14 Data processors

5.14.1 The schools shall carry out checks with prospective data processors (e.g. suppliers providing goods or services which involve the processing of personal data on the school's behalf) to assess they have appropriate technical and organisational measures that are sufficient to implement the requirements of the data protection legislation and to protect the rights of data subjects.

5.14.2 The school's Data Protection Officer and Headteacher shall assess the appropriateness of data processors before the schools purchases their services. A record will be kept of their findings.

5.14.3 The school shall ensure there are appropriate written contracts / Terms of Service in place with data processors, which contain the relevant clauses listed in Article 28 of the GDPR.

5.15 Record of processing activities

5.15.1 The schools shall maintain a record of its processing activities in line with Article 30 of the GDPR. This inventory shall contain the following information:

- Name and contact details of the school and its Data Protection Officer
- Description of the personal data being processed
- Categories of data subjects
- Purposes of the processing and any recipients of the data
- Information regarding any overseas data transfers and the safeguards around this
- Retention period for holding the data

- General description of the security in place to protect the data

5.15.2 This inventory shall be made available to the Information Commissioner upon request.

5.16 Management of personal data breaches

5.16.1 The school shall have procedures in place to identify, report, record, investigate and manage personal data breaches (i.e. security incidents involving personal data). These include security incidents resulting in the:

- unauthorised or accidental disclosure or access to personal data
- unauthorised or accidental alteration of personal data
- accidental or unauthorised loss of access or destruction of personal data

5.16.2 All security incidents and suspected personal data breaches must be reported to the Data Protection Officer immediately, by emailing simon.barker@newtown.education or telephone 01494783713.

5.16.3 All incidents will be recorded in the schools' data breach logs and investigated by a member of the Senior Leadership Team (or other person as appropriate), under the support and direction of the Federation's Data Protection Officer.

5.16.4 Notification to the ICO and Data Subjects

The Data Protection Officer shall determine whether the Federation must notify the Information Commissioner's Office and data subjects. Where a breach is likely to result in a risk to the data subject, for example if they could suffer damage, discrimination, disadvantage or distress as a result of the breach, the school (or the Data Protection Officer) shall notify the Information Commissioner's Office (ICO) within 72hrs of becoming aware of the breach.

5.16.5 If the breach is likely to result in 'high risks' to data subjects, for example if the breach could lead to identity theft, psychological distress, humiliation, reputational damage or physical harm, the school shall inform the data subject promptly and without delay.

5.16.6 When informing a data subject of a personal data breach involving their personal data, the school shall provide in clear, plain language the:

- nature of the incident
- name and contact details of the Data Protection Officer
- likely consequences of the breach
- actions taken so far to mitigate possible adverse effects

5.17 Data Protection Impact Assessments

5.17.1 The schools shall carry out Data Protection Impact Assessments (DPIAs) on all processing of personal data, where this is likely to result in high risks to the rights and freedoms of data subjects, particularly when using new technologies. This includes, but is not limited to the following activities:

- Installing and using Closed Circuit Television (CCTV)
- Collecting and using biometric information, such as fingerprints
- Sharing personal data or special category data with other organisations
- Using mobile Apps to collect or store personal data, particularly about children
- Storing special category data in the 'Cloud'
- Using systems that record large volumes of personal data, particularly where data processors are involved

5.17.2 The results from DPIAs shall be recorded and shared with the Data Protection Officer, who will advise on any privacy risks and mitigations that can be made to reduce the likelihood of these risks materialising. The Data Protection Officer will monitor the outcome of the DPIA, to ensure the mitigations are put in place.

5.18 Appointment of a Data Protection Officer

The school shall appoint a Data Protection Officer to oversee the processing of personal data within the school, in compliance with Articles 37-38 of the GDPR. This person shall be designated on the basis of professional qualities and the ability to fulfil the tasks referred to in Article 39 of the GDPR. The school shall publish the contact details of the Data Protection Officer and communicate these to the Information Commissioner's Office.

Appendix 1

Privacy notice for Parents / Carers – use of your child's personal data

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data. This privacy notice explains how we collect, store and use personal data about **pupils**.
We, Newtown School, are the 'data controller' for the purposes of data protection law.
Our data protection officer is Simon Barker (see 'Contact us' below).

The personal data we hold
Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data
We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data
We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.
Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.
Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data
We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. Our record retention schedule sets out how long we keep information about pupils. You can request a copy of this schedule from the School Office.

Data sharing
We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.
Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education – to meet legal obligations to share information with them, such as pupil details and assessments
- Parents who have parental responsibility for their child such as assessment data, progress reports attendance and behaviour analysis.
- Educators and examining bodies – for example KS1 statutory testing information
- Our regulator, Ofsted, to meet our legal obligations
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Survey and research organisations – enabling School to obtain parental views
- Health authorities, to enable them to satisfy Government Regulations and to support pupil wellbeing
- Health and social welfare organisations, where they support the welfare of individual pupils
- Professional advisers and consultants where they are contracted to support pupil wellbeing
- Police forces, courts, tribunals where there is a legal obligation to share pupil data
- Professional bodies when there is a legal obligation to share pupil data

National Pupil Database
We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census. Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.
The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.
The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.
For more information, see the Department's webpage on how it collects and shares research data.
You can also contact the Department for Education with any further questions about the NPD.

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

Parents and pupils' rights regarding personal data
Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

Parents / carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.
If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.
If you would like to make a request please contact our data protection officer.
Parents / carers also have a legal right to access to their child's **educational record**. To request access, please contact Mrs Julia Antrobus, Headteacher.

Other rights
Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints
We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with the school in the first instance.
Julia Antrobus, Headteacher, Newtown School, Berkhampstead Road, Chesham, HP5 3AT.

To make a complaint, please contact our data protection officer.
Simon Barker, Data Protection Officer, Newtown School, Berkhampstead Road, Chesham, HP5 3AT
simon.barker@newtown.education

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:
Simon Barker, Data Protection Officer, Newtown School, Berkhampstead Road, Chesham, HP5 3AT
simon.barker@newtown.education

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data in this school.

Appendix 2

Privacy notice for Newtown Staff

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data. This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.
We, Newtown School, are the 'data controller' for the purposes of data protection law.
Our data protection officer is Simon Barker (see 'Contact us' below).

The personal data we hold
We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV, application form or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving license and car insurance
- Photographs
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data
The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable equalities monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

Our lawful basis for using this data
We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

Personal data is stored in line with our data protection policy.

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment. This information is also stored on the SIMS system. Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our record retention schedule.

You may request a copy of this schedule by contacting the school office.

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law), we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about headteacher performance and staff dismissals and information for payroll purposes
- The Department for Education – to meet our legal obligation to share personal information for example for statistical and research purposes
- Your family or representatives – only in circumstances of vital interest
- Educators and examining bodies – in situations where a public task is recommended
- Our regulator, Ofsted, where there is a legal obligation to do so
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Central and local government – to meet our legal obligations
- Survey and research organisations, to enable them to provide the service we have contracted them for
- Trade unions, associations and professional bodies where there is a legitimate interest
- Health authorities where there is a vital interest
- Health and social welfare organisations where there is a legitimate interest
- Professional advisers and consultants where there is a contractual basis
- Police forces, courts, tribunals where there is a legal obligation to share personal data

Transferring data internationally

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

Your rights

How to access personal information we hold about you
Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.
If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.
If you would like to make a request, please contact our data protection officer.

Your other rights regarding your data
Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints
We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with the school in the first instance.
Julia Antrobus, Headteacher, Newtown School, Berkhampstead Road, Chesham, HP5 3AT.

To make a complaint, please contact our data protection officer.
Simon Barker, Data Protection Officer, Newtown School, Berkhampstead Road, Chesham, HP5 3AT
simon.barker@newtown.education

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:
Simon Barker, Data Protection Officer, Newtown School, Berkhampstead Road, Chesham, HP5 3AT
simon.barker@newtown.education

Appendix 3

Privacy notice for Governors and other volunteers

Under data protection law, individuals have a right to be informed about how the school uses any personal data we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data. This privacy notice explains how we collect, store and use personal data about individuals working with the school in a voluntary capacity, including Governors.
We, Newtown School, are the 'data controller' for the purposes of data protection law.
Our data protection officer is Simon Barker (see 'Contact us' below).

The personal data we hold

We process data relating to those volunteering at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- References
- Identification evidence for DBS purposes
- Evidence of qualifications
- Employment details
- Information about business and pecuniary interests

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This may include information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Disability and access requirements

Why we use this data

The purpose of processing this data is to support the school to:

- Establish and maintain effective governance
- Meet statutory obligations for publishing and sharing Governor details
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Undertake equalities monitoring
- Ensure that appropriate access arrangements can be provided for volunteers who require them

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.
Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify our use of your data.

Collecting this information

While the majority of the information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

Personal data is stored in accordance with our data protection policy.

We maintain a file to store personal information about all volunteers. The information contained in this file is kept secure and is only used for purposes directly relevant to your work with the school.

When your relationship with the school has ended, we will retain and dispose of your personal information in accordance with our record retention schedule. You can request a copy of this schedule from the school office

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Government departments or agencies – to meet our legal obligations to share information about governors
- Our local authority – to meet our legal obligations to share certain information with it, such as details of governors
- Our regulator, Ofsted, where there is a legal obligation to do so
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as governor support
- Professional advisers and consultants where there is a legitimate interest
- Police forces, courts where there is a legal obligation to share information

Transferring data internationally

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

Your rights

How to access the personal information we hold about you

Individuals have a right to make a '**subject access request**' to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have a right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints
We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with the school in the first instance.
Julia Antrobus, Headteacher, Newtown School, Berkhampstead Road, Chesham, HP5 3AT.

To make a complaint, please contact our data protection officer.
Simon Barker, Data Protection Officer, Newtown School, Berkhampstead Road, Chesham, HP5 3AT
simon.barker@newtown.education

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:
Simon Barker, Data Protection Officer, Newtown School, Berkhampstead Road, Chesham, HP5 3AT
simon.barker@newtown.education

Appendix 4

Data Protection Breach Record

Date:	
Reported by:	
Person dealing with breach:	
Date breach occurred:	
Outline of breach:	
Which data owners are involved?	
Which data types are involved?	

Phone / email sent to DPO	YES / NO	Date:
Is the breach high risk?	YES / NO	
Report to ICO	YES / NO	Date:

Actions taken following breach:	
Suggested preventative actions / suggestions:	

Completed by:	
Reviewed and signed off by:	
Date signed off:	

Appendix 5

Subject Access Request Record

Name of data subject:	
Name of person making Subject Access Request:	
Date request received:	
Date acknowledgement sent:	
Name of person dealing with request:	

Process	***Notes***
Is the requester entitled to the data?	*If no state reason and / or reply asking for evidence*
Do you understand what data they require?	*If no, ask requester for clarity*
Identify the data	*What data sources, where are they kept*
Does the school own the data?	*If no, ask third party to release data*
Does the school need to exempt / redact data?	*If redacting or excluding, be clear about the reasons*
Is the data going to be ready in time?	*Record the start and end dates and any delays*
Create data pack	*Must be in an easily accessible format*
Inform requester	*Ask requester how they would like the data delivered*
Deliver data	*Ask for confirmation of delivery*

Date request completed:	
Completed by:	
Reviewed and signed off by:	

Appendix 6

Privacy Impact Assessment Procedure

1. Introduction

A privacy impact assessment (PIA) is a tool which can help Newtown identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

An effective PIA will allow Newtown to identify and fix problems at an early project stage, reducing the associated costs and damage to reputation which might otherwise occur.

This procedure explains the principles which form the basis for a PIA.

The main body of the procedure sets out the basic steps which the school should carry out during the assessment process.

Templates are at Annex A and B

2. What is a Privacy Impact Assessment (PIA)?

A PIA is a process which helps an organisation to identify and reduce the privacy risks of any project which involves personal data. To be effective a PIA should be used throughout the development and implementation of the school's project.

A PIA will enable the school to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

3. When will a PIA be appropriate?

PIAs should be applied to all new projects, because this allows greater scope for influencing how the project will be implemented. A PIA can also be useful when planning changes to an existing system.

A PIA can also be used to review an existing system, but the school needs to ensure that there is a realistic opportunity for the process to implement necessary changes to the system. The main purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met.

Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project.

Conducting a PIA does not have to be complex or time consuming but there must be a level of rigour in proportion to the privacy risks arising. A PIA should be undertaken before a project is underway.

4. What is meant by Privacy?

Privacy, in its broadest sense, is about the right of an individual to be left alone. It can take two main forms, and these can be subject to different types of intrusion:

Physical privacy - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.

Informational privacy – the ability of a person to control, edit, manage and delete information about them and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

This procedure is concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information.

Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to someone where the person who it is about does not want them to have it;
- used in ways that are unacceptable to or unexpected by the person it is about; or
- not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information.

Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised. There is also harm which goes beyond the immediate impact on individuals. The harm arising from use of personal information may be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. It might for example contribute to a loss of personal autonomy or dignity or exacerbate fears of excessive surveillance.

The outcome of a PIA should be a minimisation of privacy risk.

5. The Benefits of a PIA

The Information Commissioner's Office (ICO) promotes PIAs as a tool which will help organisations to comply with their DPA obligations, as well as bringing further benefits.

Whilst a PIA is not a legal requirement (except 'high risk processing i.e. safeguarding data), the ICO may often ask an organisation whether they have carried out a PIA. It is often the most effective way to demonstrate to the ICO how personal data processing complies with the DPA.

More generally, consistent use of PIAs will increase the awareness of privacy and data protection issues within the School and ensure that all relevant staff involved in designing projects think about privacy at its earliest stages.

Examples of where a PIA would be appropriate

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more schools seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates information held by separate parts of the school.
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.
- Cloud hosted applications.
- The collection of new data on an existing system.

6. PIA Procedure

The format for an initial PIA is at **Appendix A.**

This review form is based on the eight Data Protection Principles described in Schedule 1 of the Data Protection Act.

In the event that a full PIA is deemed appropriate the format for this is at **Appendix B**

The links between the PIA and DPA are set out in **Appendix C**

7. Monitoring

The completed PIA should be submitted to the Governing Body for review and approval. The Governing Body will monitor implementation of actions identified in PIA's

Appendix A: (Extracted from the ICO – PIA Code of Practice)

Privacy impact assessment screening questions

These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess.

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.
- Will the project require you to contact individuals in ways that they may find intrusive?

Appendix B: (Extracted from the ICO – PIA Code of Practice)

Privacy impact assessment template

This template is an example of how to record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process that is used in this code of practice. You can adapt the process and this template to produce something that allows your organisation to conduct effective PIAs integrated with your project management processes.

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Annex C can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

Appendix C: (Extracted from the ICO – PIA Code of Practice)

Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?

How will you tell individuals about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?

If you will be making transfers, how will you ensure that the data is adequately protected?

Appendix 7

Declaration

I confirm that I have read, understood and shall adhere to Newtown School's Data Protection Policy and the supporting policies and procedures referred to in this policy.

Name:	
Job Title / Position:	
Date:	
Signature:	

Instruction for school admin
This declaration should be kept in an easily retrievable file. In the case of the school workforce in should always be kept in their personnel file.