Data Protection Policy

	Signature	Date
Chair of Governors		
Headteacher		
Committee Approval		Summer 2025
Next Review Date		Summer 2026

Contents

		Page
1	Policy Statement	1
2	Legislation	1
3	Contact	1
4	Roles and Responsibilities	1
4.1	All Staff	2
5	Data Protection Principles	3
6	Lawfulness, fairness and transparency	4
6.1	Lawfulness	4
6.2	Criminal Convictions and Offences	5
6.3	Fairness and transparency	6
7	Purpose limitation	6
8	Data minimisation	6
9	Accuracy	7
10	Storage limitation	7
11	Security	7
12	Accountability	8
13	Data Protection Impact Assessments	8
14	Sharing Personal Data	9
15	Subject Access Requests	10
15.1	Responding to subject access requests	11
15.2	Children and subject access requests	11
16	Other Data Protection Rights of the Individual	12
17	Parental Requests to access their Child's Educational Record	12
18	CCTV	12

19	Biometric Recognition Systems	13
20	Photos and Videos	14
21	Personal Data Breaches	14
21.1	Data Breach Register	15
21.2	Data Breach Response Plan	15
22	Training	15
23	Concerns and complaints	16
24	Monitoring Arrangements	16
25	Links with Other Policies and Procedures	16
26	Appendices	17

1. Policy Statement

We need to collect and use personal information so that we can operate effectively as a school and fulfil our statutory duties. The information we collect, and use includes information about pupils, parents, employees, governors, suppliers, visitors etc.

We are committed to protecting the privacy and security of this personal information at all times and supporting individuals in exercising their rights in relation to their own personal information.

This policy, along with accompanying procedures and associated policies, sets out our commitment and approach to safe data protection practice, as well as our support for individuals in exercising their rights. It applies to all personal data, regardless of whether it is in paper or electronic format.

It is reviewed annually and updated in line with any changes to data protection legislation.

2. Legislation

This policy meets the requirements of the UK General Data Protection Regulation (GDPR) and the provisions of the UK's Data Protection Act 2018.

Under the GDPR our school is classified as a Data Controller and we are registered with the UK's supervisory authority, the Information Commissioner's Office (ICO). Our registration is renewed annually.

In addition, this Policy complies with Regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record. This sits outside of the GDPR.

3. Contact

If you would like to discuss anything in this policy, please contact our Headteacher or Data Protection Officer (DPO) as follows:
Headteacher -
DPO - Nicola Cook, SchoolsDPO, nicola@schoolsdpo.com

4. Roles and Responsibilities

This policy applies to **all staff** employed by our school, as well as to external organisations or individuals working on our site.

Staff who do not comply with this policy may face disciplinary action, which could include dismissal. It is a criminal offence to access personal data held by the school for other than school business, or to procure the disclosure of personal data to a third party, or to sell such data.

The **Governing Board** has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

The **Headteacher** has overall responsibility for ensuring the implementation of this policy. They will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

The **Data Protection Officer** monitors compliance with data protection law, providing support and guidance as required.

4.1. All Staff

All Staff are responsible for ensuring that they process any personal data in accordance with this policy (a definition of processing can be found in Appendix 1). Staff must also inform the office of any changes to their personal data, such as a change of address.

Staff must contact the office whenever they have a query about data protection, including, but not limited to the following:

- any questions about the operation of this policy: including retaining personal data; keeping personal data secure; sharing personal data with third parties; or whether there is a lawful basis in place for a particular data processing operation
- any concerns that the policy is not being followed
- a new project under consideration that involves the processing of personal data
- received any requests from individuals for access to their personal information the school is processing.

5. Data Protection Principles

The UK GDPR sets out seven key principles which form the foundation of this data protection legislation:

- **Lawfulness, fairness and transparency** - Data shall be processed lawfully, fairly and in a transparent manner in relation to individuals

- **Purpose limitation** - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

- **Data minimisation** - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

- **Accuracy** - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

- **Storage limitation** - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest; scientific or historical research purposes or statistical purposes. This is subject to implementation of the appropriate technical and organisational measures required by the GDPR, in order to safeguard the rights and freedoms of individuals

- **Integrity and confidentiality (security)** - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

- **Accountability** - the controller shall be responsible for, and able to demonstrate, accountability with the GDPR principles.

This **Data Protection Policy**, along with our privacy notices and additional policies and procedures referenced in section 25, sets out how our school aims to comply with these principles.

6. Lawfulness, fairness and transparency

6.1. **Lawfulness**

We will always ensure we have a valid lawful basis for our processing of personal data. There are six lawful bases we can rely on under the UK GDPR:

- **Contract** - the processing is necessary for a contract with an individual, or because they have asked for specific steps to be taken before entering into a contract.

- **Legal obligation** - the processing is necessary to comply with the law (not including contractual obligations).

- **Vital interest** - the processing is necessary to protect someone's life.

- **Public task** - the processing is necessary to perform a task in the public interest or for our official functions as a school, and the task or function has a clear basis in law.

- **Legitimate interests** - the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

- **Consent** - the individual has given clear and informed consent for their personal data to be processed for a specific purpose. The individual can change their mind at any time and withdraw their consent. If this happens the processing will be stopped.

Some personal data is considered more sensitive under the GDPR, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric information (such as fingerprints, retina and iris patterns), where used for identification purposes, health – physical or mental, sex life or sexual orientation.

For these **special categories** of personal data, we will also identify one of the special category conditions for processing set out in the GDPR:

- Explicit consent
- Employment, social security and social protection (if authorised by law)
- Vital interests
- Not-for-profit bodies
- Made public by the data subject
- Legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Health or social care (with a basis in law)
- Public health (with a basis in law)
- Archiving, research and statistics (with a basis in law).

In addition, under the UK's Data Protection Act 2018, we rely on the processing conditions at Schedule 1 part 1, paragraphs 1, 8 and 18. These relate to the processing of special category data for employment purposes, safeguarding and equality of opportunity/treatment.

Our Appropriate Policy Document provides more information about this processing. This can be found on the school website and on the shared drive.

6.2. Criminal Convictions and Offences

The UK GDPR also gives extra protection to **criminal offence data**. As well as ensuring a valid lawful basis for the processing of criminal offence data under the GDPR, we will also identify an additional condition set out in Schedule 1 of the UK DPA 2018.

Under Article 6 of the GDPR, lawful bases we rely to process this data are:

- Performance of our **public task**
- Performance of a **contract**.

In addition, under the UK's Data Protection Act 2018, we rely on the processing conditions at Schedule 1:

- Part 2, para 6(2)(a)
- Part 1, para 1.

These relate to the processing of criminal offence data for statutory and employment purposes respectively. See Part 3 of *Keeping Children Safe in Education* for more information.

Our Appropriate Policy Document provides more information about this processing.

6.3. Fairness and transparency

Data protection legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by the GDPR.

This will normally be through our **privacy notices**:

Our **Privacy Notice for Pupils and Parents** sets out how we process pupil personal data to support teaching and learning, to provide pastoral care and to assess the performance of our services.

Our **Privacy Notice for Staff** sets out how we process the personal data of staff, agency staff and contractors to fulfil our obligations as an employer.

Our **Privacy Notice for Governors and Volunteers** sets how we process governors' and volunteers'personal data to support them in fulfilling their governance role.

All our Privacy Notices also include information on the rights of the individuals whose data we are processing and who to contact to discuss any aspect further.

7. Purpose limitation

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to individuals when we first collect their data (usually through our privacy notices).

If we want to use personal data for reasons other than those given when we first obtained it, we will identify and document a new lawful basis; although this may not be necessary if our new purpose is compatible with the original purpose. We will inform the individuals concerned before we do so, and seek consent where necessary.

8. Data minimisation

We will only collect the minimum amount of personal data necessary for our purposes. Staff will only process personal data where it is necessary to perform their roles.

9. Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs us of a change of circumstances, their records will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, we will immediately

mark the record as potentially inaccurate, or “challenged”.

10. Storage limitation

When our school no longer needs the personal data it is processing, it will be deleted or anonymised. This will be done in accordance with our data retention schedule. This can be found on our school website and in the shared drive.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use an outside company to convert paper records to electronic files and shred documents.

Where details of individuals are stored for long-term archive, historical or statistical reasons, this will be done within the requirements of the GDPR.

11. Security

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

All members of staff are required to sign to confirm that they have read and understood this Data Protection Policy.

All members of staff are required to sign an acceptable user agreement which is renewed annually. The acceptable user agreement is linked to the school’s E-safety Policy and covers such aspects as:

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information being kept securely when not in use
- Papers containing personal information being kept secure and not being left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access
- Staff ensuring that individual monitors do not show confidential information to passers-by and that they log off from their device when it is left unattended
- Staff adhering to school policies and procedures when taking data off site and when working remotely or at home
- Strong passwords being used to access school systems, online resources, laptops and other electronic devices. These must be at least 8 characters long containing letters and numbers; or preferably passphrases (e.g. 3 unconnected words).
- Encryption software being used to protect all portable devices and removable media
- Staff not storing personal information on their personal devices and being expected to follow the same security procedures as set out for any school owned equipment
- GDPR compliant cloud storage being used for all online data storage
- The use of USB devices not being allowed to store personal data.

12. Accountability

The school has put in place appropriate technical and organisational measures to meet the requirements of the accountability principle These include:

- The appointment of a data protection officer who reports directly to our highest management level
- Taking a 'data protection by design and default' approach to our activities
- Maintaining accurate documentation of our processing activities, such as the purposes of processing personal data, data sharing and retention. We also document the lawful bases and conditions we are relying on for our purposes, including how and when consent was obtained, as appropriate
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors
- Implementing appropriate security measures in relation to the personal data we process
- Carrying out data protection impact assessments for our high risk processing (see section 6).

We regularly review our accountability measures and update or amend them when required.

13. Data Protection Impact Assessments

The GDPR requires us to carry out Data Protection Impact Assessments (DPIAs) for any type of processing that is likely to result in a high risk to individuals' interests; for example, when introducing new technologies, or using biometric data for identification purposes.

To assess the level of risk, we consider both the likelihood and the severity of any impact on individuals. High risk can result from either a high probability of some harm, or a lower possibility of serious harm.

If we identify a high risk that we cannot mitigate, we will consult the ICO before starting the processing.

As part of our data protection by design and default approach we will carry out a DPIA for any other major project which requires the processing of personal data.

We follow the ICO's guidelines and our DPIAs:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks.

14. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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

Where we transfer personal data to a country or territory outside the United Kingdom, we will do so in accordance with the international transfer rules in the GDPR .

Where we share personal data on an ad hoc or ‘one off’ basis, we will record the details including our purpose and lawful basis for doing so.

15. Subject Access Requests

Under the GDPR, anyone whose personal data we are processing, e.g staff, pupils and parents\carers etc, has a right to make a ‘subject access request’ to gain access to information our school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data

- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests can be made by contacting any member of staff, but it is helpful if they are made to the School Office or the DPO. They can be made in person, verbally, in writing, and by email. The following information will be required:

- Name of individual
- Relationship of the requester to the individual, if appropriate
- Correspondence address
- Contact number and email address
- Details about the information requested

Completion of a subject access request form can be useful, but this cannot be insisted upon.

If a member of staff receives a subject access request they must immediately forward it to the School Office.

Members of staff can find further information on their role in handling subject access requests in our Guidance for Staff.

15.1. Children and Subject Access Requests

A child's personal data always belongs to them rather than the child's parents or carers.
For a parent or carer to make a subject access request, with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent. The UK's Information Commissioner's Office generally regards children aged 12 and above to be mature enough to understand their rights and the implications of a subject access request. However, we will always consider this on a case by case basis.

15.2. Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification, if necessary

- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not reveal the following information in response to Subject Access Requests:

- Information that might cause serious harm to the physical or mental health of the subject or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child
- Any references that have been provided or received in confidence.

If the request is considered unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be considered to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

16. Other Data Protection Rights of the Individual

In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it (see section 6), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the United Kingdom
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances

- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

If staff receive such a request, they must immediately forward it to the school office.

17. Parental Requests to access their Child's Educational Record

In maintained schools, parents have a separate right to access their child's educational record under the Education (Pupil Information, England) Regulations 2005. The request must be made in writing and the information will be provided within 15 school days of receipt of the request.

18. Photos and Videos

As part of our educational activities, we may take photographs and record images of individuals. We will always clearly explain to pupils and/or parents (as appropriate) how the photograph or video will be used.

We will obtain consent for photographs and videos to be taken of pupils for marketing and promotional materials.

Uses may include:

- In school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media page.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the individual, to ensure they cannot be identified.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

19. Personal Data Breaches

The GDPR defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

When a personal data breach has occurred we will assess the likelihood and severity of the resulting risk to the rights and freedoms of the individuals involved. If it's likely that there will be a risk, then we are required by law to notify the ICO.

19.1. Data Breach Register

We record all breaches of personal data, regardless of whether they are reported to the ICO. Our data breach register includes the details of the breach, its effects and any remedial action taken. Remedial action may include a review of relevant systems or policies and procedures; additional training for staff; or other corrective steps, as appropriate.

19.2. Data Breach Response Plan

Each breach will be considered on a case by case basis and our Data Breach Response Plan sets out in more detail the procedures we will follow. Please see appendix 1.

If any member of staff believes a breach of personal data has occurred, or might have occurred, they are required to let the headteacher know immediately.

20. Training

Our staff are provided with data protection training as part of their induction process and this is refreshed at least annually. We take a blended approach, so training may be formal CPD - face to face or online delivery; through INSET days, staff meeting updates and discussion, 1:1 reviews, newsletters etc.

Uptake of training is monitored and procedures are in place to ensure that all staff complete the required training.

21. Concerns and Complaints

We will always endeavour to resolve any concerns an individual may have about our processing of their personal data informally. However, if this is not possible, the individual will be advised to use our school's complaints procedure. If, after this, the individual remains concerned, they will be advised how they can raise those concerns with the ICO.

22. Monitoring Arrangements

The Governing Board is responsible for monitoring and reviewing this policy. It will be reviewed on an annual basis.

23. Links with Other Policies and Procedures

This Data Protection Policy is linked to:

- Privacy Notice for Pupils and Parents
- Privacy Notice for Staff
- Privacy Notice for Governors and Volunteers
- Acceptable User Agreements
- Record Retention Schedule
- Data Breach Response Plan
- Appropriate Policy Document
- E-safety Policy
- Child Protection Policy/Safeguarding Policy
- Freedom of Information Publication Scheme.

Appendix 1
Newtown School Data Breach Response Plan

1. Introduction

This data breach response plan sits is an appendix to our school's Data Protection Policy which it should be read in conjunction with. If you have any queries, please contact Hayley England our Data Protection Lead in the first instance.

The General Data Protection Regulation (GDPR) defines a personal data breach as:

"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."

A breach of personal data is a type of security incident and falls into one of three categories:

- "Confidentiality breach" - an unauthorised or accidental disclosure of, or access to, personal data
- "Integrity breach" - an unauthorised or accidental alteration of personal data
- "Availability breach" - an accidental or unauthorised loss of access to, or destruction of personal data.

A breach may concern the confidentiality, integrity and availability of personal data at the same time, or any combination. It can be the result of both accidental and deliberate causes.

Some examples of personal data breaches include:

- access by an unauthorised third party (including the malicious acts of hackers and scammers)
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing/mobile devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data, e.g. when it has been encrypted by ransomware, or accidentally lost or destroyed (including natural disasters such as fire and flood).

Under the GDPR any breach of personal data requires mandatory notification to our supervisory authority, the Information Commissioner's Office (ICO); unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

2. When a Breach of Personal Data Occurs

As soon as we are aware* that a breach of personal data has occurred, we will immediately seek to contain the incident and also assess the risk to the rights and freedoms of the individual(s) involved.

*Awareness of a breach occurs when we have a reasonable degree of certainty that a breach has occurred.

The GDPR requires us to use our resources to ensure we are 'aware' of a data breach in a timely manner. In some cases it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised.

A data incident/breach may occur during school holidays when the school is closed or we have a reduced number of staff available. We will ensure that all members of staff have the contact details of the Data Protection Lead and DPO so that any incident/breach can still be dealt with appropriately. These contact details are also included in our Data Protection Policy and Privacy Notices, which are available on our website.

3. Assessment of Risk

The risk from a breach is assessed on a case by case basis and both the severity of the potential impact on the rights and freedoms of the individuals and the likelihood will be considered.

When assessing the risk to individuals as a result of a personal data breach we will consider:

- The type of breach
- The nature, sensitivity and volume of the personal data
- How easy it is to identify individuals
- The severity of consequences for individuals
- Special characteristics of the individual, e.g. if they are children
- Any special characteristics of our school
- The number of affected individuals.

A breach is likely to result in a risk to the rights and freedoms of individuals if it could result in physical, material or non-material (e.g.emotional) damage. In particular:

- Loss of control over personal data
- Limitation or deprivation of individuals' rights
- Discrimination
- Identity theft or fraud
- Financial loss
- Damage to reputation
- Unauthorised reversal of pseudonymisation
- Loss of confidentiality of personal data protected by professional secrecy
- Any other significant economic or social disadvantage.

Where special category data* is involved, the GDPR states that such damage should be considered to be likely to occur.

*Special category data is data that is considered more sensitive and requires greater protection: racial or ethnic origin, political opinion, religion or philosophical beliefs, trade union membership, genetic data, data concerning health or sex life, or biometric data used for identification purposes. Data relating to criminal convictions is afforded similar special protection.

4. Notification to the ICO

As a result of this assessment, if we believe that there is a risk to the rights and freedoms of the individual(s), we will notify the Information Commissioner's Office, as required under the GDPR. If we are in any doubt, we will always err on the side of caution and notify the ICO.

Where we assess a breach is reportable to the ICO, we must make this report without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach.

As a minimum, we must include in our notification:

- description of the nature of the personal data breach including, where possible:
    - categories and approximate number of individuals concerned
    - categories and approximate number of personal data records concerned
- name and contact details of the DPO
- description of the likely consequences of the personal data breach
- description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

The GDPR makes no allowance in the statutory reporting timescale of 72 hours for breaches that occur during school holidays. Therefore, it is important that staff contact the school Data Protection Lead and the DPO as soon as possible.

5. Communication to affected individuals

Where a data breach is likely to result in a high risk to the rights and freedoms of individuals, we will notify affected individuals as soon as possible. We will provide:

- A description of the nature of the breach
- The name and contact details of the DPO and/or Data Protection Lead
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to be taken, by the school to address the breach and mitigate any possible adverse effects.

We will also consider what specific advice we can provide to individuals to help them protect themselves, such as resetting passwords where access credentials have been compromised.

6. Roles and Responsibilities

All Staff - if any member of staff believes a breach of personal data has occurred, or might have occurred, they must immediately notify the Data Protection Lead, Hayley England Hayley.england@newtown.education who will liaise with the Data Protection Officer:
Nicola Cook, SchoolsDPO Ltd:
01296 658502, nicola@schoolsdpo.com.

If members of staff receive personal data sent in error they must alert the sender and the **Data Protection Lead** as soon as they become aware of the error.

The **Data Protection Lead**, with the support of colleagues, will investigate the report, and determine whether a breach has occurred. To decide, they will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed, or made available where it should not have been
- Made available to unauthorised people.

The **Data Protection Lead** will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

In discussion with the **Data Protection Lead**, the **DPO** will assess the potential consequences of the breach and advise whether the breach needs to be reported to the ICO.

If the breach is likely to be a risk to the people's rights and freedoms, the **DPO** will notify the ICO.

Where a breach is likely to result in a high risk to people's rights and freedoms, the **Data Protection Lead** will promptly inform, in writing, all individuals whose personal data has been breached. This notification will include:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

- The **Data Protection Lead** will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The **Data Protection Lead** will document each breach, irrespective of whether it is reported to the ICO and ensure a record is kept in the Data Breach Register.

7. Actions to minimise the impact of data breaches

The type of action we might take will depend on the nature of the breach, but could include (this list is not exhaustive):

- Attempting to recover lost equipment
- Remotely wiping electronic devices
- Using of back-ups to restore lost/damaged/stolen data
- Changing entry codes or IT system passwords
- Attempting to recall emails containing personal information that are sent to unauthorised individuals
- Requesting personal data received in error is deleted and written confirmation is provided that the information has been deleted, and not shared, published, saved or replicated in any way
- Carrying out internet searches to check information hasn't been made public. If it has, asking the publisher/website owner/administrator to remove and destroy the information
- Briefing staff in case of phishing enquiries for further information on affected individuals
- Notifying the Local Authority.

We will review the effectiveness of any actions taken and amend them as necessary after any data breach. This may include establishing more robust policies and procedures or providing further training for staff.

8. Accountability and Record Keeping

We record all breaches of personal data regardless of whether they are reported to the ICO. This helps us demonstrate our compliance with the GDPR under its principle of accountability. It also ensures we have records should the ICO wish to see them.

Our data breach register includes:

- Summary of the facts:
  - including the types and amount of personal data involved
  - details of the cause of the breach and impact on the individuals whose data is involved
- Actions taken to contain the breach as well as mitigate its possible adverse effects
- Any actions taken to prevent future breaches.

24. Appendix 2 - Definitions

Term	Definition
Personal data	Data from which a person can be identified (i.e. distinguished from other individuals); such as: • Name (including initials) • Identification number • Location data • email address, telephone number, car registration number • Online identifier, such as a username, IP addresses, cookie identifiers • photographs, video recordings This includes data that, when combined with other readily available information, leads to a person being identified.
Special category persona data	Personal data which is more sensitive and is therefore afforded more protection under the GDPR. Data such as: • Racial or ethnic origin • Political opinions • Religious beliefs, or philosophical beliefs • Where a person is a member of a trade union • genetic data • biometric data (when used for identification purposes) • Physical and mental health • Sexual orientation and sex life Data relating to criminal convictions is afforded similar special protection.
Processing	Any operation carried out on personal data, such as collecting, recording, storing,altering, retrieving, using, disseminating,erasing or destroying. Processing can be automated or manual.
Data subject	The living individual whose personal data is held or processed.

Data controller	A person, or organisation, that determines the purpose for which, and the way, personal data is processed.
Data processor	A person, or other body, other than an employee of the data controller, who processes the data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Breaches can be the result of accidental or deliberate causes.

Appendix 3

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 Nicola Cook (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.
Hayley England, Headteacher, Newtown School, Berkhampstead Road, Chesham, HP5 3AT.

To make a complaint, please contact our data protection officer.
Nicola Cook, Data Protection Officer, Newtown School, Berkhampstead Road, Chesham, HP5 3AT
nicola@schoolsdpo.com

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**:
Nicola Cook, Data Protection Officer, Newtown School, Berkhampstead Road, Chesham, HP5 3AT
nicola@schoolsdpo.com

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 4

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 Nicola Cook (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.
Hayley England, Headteacher, Newtown School, Berkhampstead Road, Chesham, HP5 3AT.

To make a complaint, please contact our data protection officer.
Nicola Cook, Data Protection Officer, Newtown School, Berkhampstead Road, Chesham, HP5 3AT
nicola@schoolsdpo.com

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**:
Nicola Cook, Data Protection Officer, Newtown School, Berkhampstead Road, Chesham, HP5 3AT
nicola@schoolsdpo.com

Appendix 5

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 Nicola Cook (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.
Hayley England, Headteacher, Newtown School, Berkhampstead Road, Chesham, HP5 3AT.

To make a complaint, please contact our data protection officer.
Nicola Cook, Data Protection Officer, Newtown School, Berkhampstead Road, Chesham, HP5 3AT
nicola@schoolsdpo.com

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**:
Nicola Cook, Data Protection Officer, Newtown School, Berkhampstead Road, Chesham, HP5 3AT
nicola@schoolsdpo.com

Appendix 6

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 7

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 8

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.