Test Valley SCHOOL

"In Pursuit of Personal Excellence"

Head of School: Ms Caroline Lowing

Initial Policy date	November 2022	Next scheduled review	November 2023
Governor approved	16 November 2022	Key person/people	Business Manager
Model Policy	Y	Model localised	
Pupil leadership team review		~~Y /~~ N ~~/ N/A~~	

DATA PROTECTION POLICY/GDPR

Our aims are to:

Data Protection falls within the scope of the Data Protection Act (DPA) 2018, which sits alongside the General Data Protection Regulation (GDPR), and tailors how GDPR applies in the UK. This policy follows the recommendations issued by the Data Protection Commissioner in accordance with powers under the 2018 Act.

Contents.

1. Legislation and guidance 2
2. Definitions 2
3. The data controller 3
4. Roles and responsibilities 3
5. Data protection principles 4
6. Collecting personal data 4
7. Sharing personal data 5
8. Subject access requests and other rights of individuals 6
9. Parental requests to see the educational record 8
10. Biometric recognition systems 8
11. CCTV 8
12. Photographs and videos 9
13. Data protection by design and default 9
14. Data security and storage of records 9
15. Disposal of records 10
16. Personal data breaches 10
17. Training 11
18. Monitoring arrangements 11
19. Links with other policies 11

Appendices:

Appendix One: Data Protection Responsibilities – For All Staff.

Appendix Two: DPO's Roles and Responsibilities.

Appendix Three: Checklist for seeking consent to process personal data.

Appendix Four: Third-Party Data Agreement.

Appendix Five: Subject Access Request form.

Appendix Six: Use of Biometric Data – Consent Form.

Appendix Seven: Consent form for taking and using photos/ videos and social media..

Appendix Eight: Data Privacy Impact Assessment template.

Appendix Nine: Pupil Privacy Notice.

Appendix Ten: Privacy Notice.

Appendix Eleven: Colleague Privacy Notice.

Appendix Twelve: Personal Data breach procedure.

Appendix Thirteen: Data Breach Reporting Form.

1. Legislation and guidance.

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

- The requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.
- It reflects the ICO's code of practice for the use of surveillance cameras and personal information.
- In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.
- DfE Data protection: a toolkit for schools April 2018.

2. Definitions.

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username

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

3. The data controller.

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

The school is registered as a data controller with the ICO (Registration reference: Z6454920) and will renew this registration annually or as otherwise legally required.

4. Roles and responsibilities.

This policy applies to **all staff** employed at Test Valley School, volunteers and external organisations or individuals working on our behalf. Colleagues who do not comply with this policy (with attention to Appendix One: Data Protection Responsibilities – For All Staff) may face disciplinary action, in accordance with the school (Model) Code of Conduct Policy.

4.1 Governing body.

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection and with demonstrating their commitment to these obligations. All Governors are issued with individual school email accounts, which are to be used when dealing with school Data. The clerk of Governors is to arrange the necessary requirements as part the induction and end of tenure process.

4.2 Data protection officer.

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

They will provide a report of their activities directly to Governors Finance Committee and, where relevant, report to the Full Governing Body for their advice and recommendations on school Data Protection issues.

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

Full details of the DPO's Roles and Responsibilities can be found at Appendix Two.

Details of our DPO is displayed on the school website and is contactable via office@testvalley.hants.sch.uk

4.3 Headteacher.

The headteacher acts as the representative of the data controller on a day-to-day basis.

4.4 All staff.

All colleagues working at Test Valley School and volunteers, have a personal responsibility to keep person identifiable information and sensitive school information secure and confidential always:

Key Staff Data protection responsibilities are outlined at Appendix One.

5. Data protection principles.

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes and not in any manner incompatible with those purposes
- Adequate, relevant and not excessive
- Accurate
- Kept for no longer than is necessary
- Processed in accordance with individuals'' rights
- Secure

This policy sets out how the school aims to comply with these principles and applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

6. Collecting personal data

6.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**. A checklist for seeking consent to process personal data, can be found at Appendix Three.

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

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

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

6.2 Limitation, minimisation and accuracy.

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

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Local Authority School Records Retention Schedule Retention Policy.

7. 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 any person at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share. An example of our Third-Party Data Agreement can be found at Appendix Four
- 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 that affects any of our pupils or staff.

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

8. Subject access requests and other rights of individuals

8.1 Subject access requests

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

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

It will be easier to recognise and respond to requests if they are in a consistent format, therefore Subject Access Requests must be submitted in writing, and using the template at Appendix Five: Subject Access Request form will greatly assist this process. This can then be emailed to the DPO, or alternatively it can be handed into the main office. Forms should include:

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

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

8.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

8.3 Responding to subject access requests

When responding to requests, we:

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

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

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

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

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

8.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 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 based on public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area

- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

9. Parental requests to see the educational record

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

10. Biometric recognition systems

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

Parents/carers will be notified regarding our biometric recognition system. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it. This can be found at Appendix Six: Use of Biometric Data – Consent Form.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

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

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent, and provide the alternative means mentioned above, if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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

Any enquiries about the CCTV system should be directed to the DPO.

12. Photographs and videos

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

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and 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 pages

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 child, to ensure they cannot be identified.

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

Our consent form for taking and using photos/ videos – can be found at Appendix Seven.

13. Data protection by design and default

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

- A suitably qualified DPO, has been appointed, who will have the necessary resources to fulfil their duties and maintain their knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing Data Privacy Impact Assessments (DPIA) where the school's processing of personal data presents an elevated risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process). Our Privacy impact assessment template can be found at Appendix Eight
- Integrating data protection into internal documents including this policy, any related policies. Our Privacy notices, which will be displayed on the school website can also be found at:
    - Appendix Nine: Pupil Privacy Notice
    - Appendix Ten: Parent Privacy Notice
    - Appendix Eleven: Colleague Privacy Notice
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how

and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Staff are to ensure confidential information is shredded when no longer needed. Shredding bags must also be secured.
- Care must be taken to ensure pupil information is not accidently displayed on screens
- Where personal information needs to be taken off site, staff must sign it in and out from the school office, or medical room
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software/ devices is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our online safety policy/ICT policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 7)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

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

In the unlikely event of a suspected data breach, we will follow the Personal Data Breach Procedure set out in Appendix Twelve.

When appropriate, we will report the data breach to the ICO within 72 hours, by calling the helpline 0303 123 1113 or out of hours completing their online form, Appendix 13. Such breaches in a school context may include, but are not limited to:

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

17. Training

All staff and governors are provided with data protection e learning training as part of their induction process.

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

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy and procedure. Major changes will be bought to the Governing body, if this is prior to the annual review.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Safeguarding policies
- Retention
- School (Model) Code of Conduct Policy
- CCTV
- Online safety policy/ICT policy

Appendix One

Data Protection Responsibilities – For All Staff.

All colleagues working at Test Valley School and volunteers have a personal responsibility to keep person identifiable/ sensitive information secure and confidential always:

Key responsibilities:

- Under GDPR colleagues should be doing everything to prevent a breach of personal Data
- Ensuring the security of personal data access from own devices:
    - Such as laptops or phones, to prevent the data from being lost, stolen or accidentally leaked.
    - Colleagues are not to share any devices that store personal data among family and friends.
    - Make sure antivirus software is installed on personal laptops and computers. Keep it up to date and ensure it makes regular scans.
- Keep the device password-protected:
    - All devices should be locked using a strong password or a PIN, to prevent others from accessing data through them
    - Strong passwords are at least 7 characters, with a combination of upper and lower-case letters, numbers and special keyboard characters (e.g. an asterisk or currency symbols)
    - If a wrong password or PIN is entered too many times, access to the device should be locked, or data stored in it should be automatically deleted
- Staff, pupils and contractors are not permitted to introduce or use any removable media, such as memory stick or hard drives, unless it is an **encrypted** device, with considerable care taken for its security
- Teaching colleagues must take care to ensure that pupils' information is not accidently displayed on screens in classrooms, eg tutor registration
- Do not open any hyperlinks in emails or any attachments to emails, unless the source is known, trusted and expected
- Careful consideration will still need to be given with regards to why, whose, what and where the email is being sent - particularly when this pertains to personal information
- Locking computers. Accounts must be locked when moving away from a logged in terminal when left unattended, even for short periods of time - to prevent unauthorized access
- Collecting, storing and processing any personal data on school IT systems in accordance with this policy; colleagues must only process personal data, including photos, where it is necessary to do their jobs
- When staff no longer needs the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Local Authority School Records Retention Schedule Retention Policy.
- Staff must Inform the school of any changes to their personal data, such as a change of address, as soon as possible
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data must be kept secure when not in use. Staff must ensure that confidential info is shredded when no longer needed. Shredding bags must also be secured.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from either the school office or medical room (eg medical care plans)
- Contact the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If there are any concerns that this policy is not being followed
- If colleagues are unsure whether they have a lawful basis to use personal data in a certain way
- If colleagues need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach or, potential breach
- Whenever they are engaging in a recent activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties
- Application of standalone learning application requiring a third-party Data processor
- On receipt of any Subject Access Requests – an example of which is a pupil's behaviour record – these must be handled through the HT and DPO
- All members of staff must also be aware of potential data breaches occurring using social media and must refer to the schools 'safer use of IT policy' in conjunction with this policy

Appendix Two

DPO's Roles and Responsibilities.

Purpose.

The DPO is responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee the school's data protection processes and advise the school on best practice.

Key responsibilities:

- Advise the school and its employees about their obligations under current data protection law, including the General Data Protection Regulation (GDPR)
- Develop an in-depth understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures
- Monitor the school's compliance with data protection law, by:
    - Collecting information to identify data processing activities
    - Analysing and checking the compliance of data processing activities
    - Informing, advising and issuing recommendations to the school
    - Ensuring they remain an expert in data protection issues and changes to the law, attending relevant training as appropriate
- Ensure the school's policies are followed, through:
    - Assigning responsibilities to individuals
    - Awareness-raising activities
    - Co-ordinating staff training
    - Conducting internal data protection audits
- Advise on and assist the school with carrying out data protection impact assessments, if necessary
- Act as a contact point for the Information Commissioner's Office (ICO), assisting and consulting it where necessary, including:
    - Helping the ICO to access documents and information
    - Seeking advice on data protection issues
- Act as a contact point for individuals whose data is processed (for example, staff, pupils and parents), including:
    - Responding to subject access requests
    - Responding to other requests regarding individuals' rights over their data and how it is used
- Take a risk-based approach to data protection, including:
    - Prioritising the higher-risk areas of data protection and focusing mostly on these
    - Advising the school if/when it should conduct an audit, which areas staff need training in, and what the DPO role should involve
- Report to the governing body on the school's data protection compliance and associated risks
- Respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role
- Undertake any additional tasks necessary to keep the school compliant with data protection law and be successful in the role
- Maintain a record of the school's data processing activities
- Work with external stakeholders, such as suppliers or members of the community, on data protection issues

- Take responsibility for fostering a data protection culture throughout the school. Work closely with other departments and services to ensure GDPR compliance, such as HR, legal, IT and security

Appendix Three

A checklist for seeking consent to process personal data.

Action	
Deciding whether you need to seek consent	
We have checked that consent is the most appropriate lawful basis for processing. The School only needs to seek consent where none of the other lawful bases apply. For example, ask for consent to: • Using photographs or videos of pupils on your school's website or other promotional material • Sending marketing material to prospective parents • Sending fundraising requests to alumni • Use of Biometrics Examples where consent is not required as it is covered by our other 'lawful bases' (legal reasons) to do so under data protection law, are: • Sharing child protection concerns and records with the appropriate people or agencies (a specific document is used for police requests) • Submitting census data to the Department for Education	
Asking for consent (refer to these actions when writing a consent form)	
We have made the request for consent clear and separate from other terms and conditions	
We ask people to positively opt in	
We don't use pre-ticked boxes, or any other type of consent by default	
We use clear, plain language that is easy to understand	
We specify why we want the data and what we're going to do with it	
We give separate options to consent to the different things we will do with the data For example, if you're asking for consent to take photographs of children, ask parents to agree to each thing the photograph will be used for: "I am happy for the school to take photographs of my child. I am happy for photos of my child to be used on the school website. I am happy for photos of my child to be used in the school prospectus"	
We have named our organisation and any third parties that process the data	
We tell individuals they can withdraw their consent	

We ensure that the individual can refuse to consent without detriment	
We don’t make consent a precondition of a service	
Recording consent	
We keep a record of when and how we got consent from the individual	
We keep a record of exactly what they were told at the time	
Managing consent on an ongoing basis	
We regularly review consents to check that the relationship, the processing and the purposes have not changed	
We have processes in place to refresh consent at appropriate intervals, including any parental consents	
We make it easy for individuals to withdraw their consent at any time, and publicise how to do so	
We act on withdrawals of consent as soon as we can	
We don’t penalise individuals who wish to withdraw consent	

Appendix Four

Third-Party Data Agreement.

Data Protection Contract Clauses for Test Valley School – Third Party agreement.

1. The Supplier shall ensure that its staff, representatives and agents comply with the requirements of the Data Protection Act 1998 and the General Data Protection Regulation and any successor legislation (the Data Protection Legislation) when collecting or using the personal or special category data for the provision of the Services and shall not knowingly or negligently place the School in breach, or potential breach, of the Data Protection Legislation.

2. The Supplier is permitted to collect and use the following data but only to the extent necessary for the provision of the Services and only in accordance with documented instructions from the School and for no other purpose whatsoever except as required by law to act without such instructions ***(see Note 1 below)***:-

Personal Data	Special Category Data
Names	*Racial / ethnic origin*
Addresses	*Political opinions*
Email addresses	*Religious or philosophical beliefs*
Telephone number	*Trade union membership*
	Genetic data
	Biometric data
	Health data
	Data concerning sex life or sexual orientation

3. The Supplier is only permitted to collect and use the information described in clause 2 in respect of the following data subjects ***(see Note 2 below)***:-

- Pupils
- Parents
- School Staff
- Visitors
- Professional advisers

4. The Supplier shall obtain specific prior written authorisation from the School before engaging a subcontractor to provide any of the Services and shall oblige that subcontractor to fully comply with the requirements of the Data Protection Legislation imposing the same data protection obligations within the subcontract as are contained in this Contract.

5. No personal information shall be disclosed to any other third party without first consulting the School regarding the legality and mechanism of the disclosure and obtaining the School's written authorisation confirming it is satisfied that there is a legal basis permitting the disclosure of the data, and that the disclosure mechanism is appropriate.

6. On termination of this Contract the Supplier shall return all personal data to the School or destroy or dispose of it in a secure manner and in accordance with any specific instructions issued by the School and shall confirm to the School that it has done so.

7. The Supplier shall give all reasonable assistance to the School necessary to enable the School to comply with its obligations under the Data Protection Legislation.

8. The Supplier shall comply with the School's security requirements and instructions, and shall have appropriate technical and organisation safeguards in place to protect the data and to meet the obligations imposed on it and the School by the Data Protection Legislation.

9. The Supplier shall, upon reasonable notice, allow officers of the School or an auditor appointed by the School, to have reasonable rights of access to the Supplier's premises, staff and records for the purposes of monitoring the Supplier's compliance with its security requirements and with the Data Protection Legislation.

10. The Supplier shall take reasonable steps to ensure the reliability of its staff accessing the School's data and shall ensure that they receive appropriate training in data protection to understand the confidential nature of the data and the need to comply with Data Protection Legislation. The Supplier shall ensure that it, its staff, representatives, agents and visitors will not access, read, listen to or in any way use School data unless it is necessary to do so for the provision of the Services and they have committed themselves to confidentiality.

11. The Supplier shall ensure that no personal data is transferred to a country or territory outside the European Economic Area and that no other data is transferred to a country or territory outside the European Economic Area without the prior written authorisation of the School.

12. The Supplier agrees to indemnify the School against all costs, claims and liabilities incurred by the School as a result of the Supplier's and / or the Supplier's Subcontractor's failure to comply with Data Protection Legislation as required by this Contract.

13. The Supplier shall notify the School within 24 hours if it becomes aware of a breach or potential breach of Data Protection Legislation.

14. In the event that the Supplier fails to comply with these terms, the School reserves the right to terminate this Contract, in whole or in part, in writing with immediate effect.

Note 1 *– The GDPR requires that types of personal data to be processed must be set out in contracts between data controllers and data processors (in most cases a school will be a data controller and a supplier will be a data processor). Please list the type of personal data which will be accessed and used in any way by the Supplier under the contract. You will need to delete any that are not relevant from the examples provided. For special category data, we suggest you simply list the data processed by the Supplier by reference to the categories only (as shown in the examples) and delete any that are not applicable.*

Note 2 *– The GDPR requires that categories of data subjects whose personal data is to be accessed and used by the supplier are listed in the contract. Please add to or delete the categories of data subjects as applicable.*

School:	***Third Party***
	Name:
Data Protection Officer, on behalf of HT	*Appointment:*
Test Valley School	*Company/ Organisation:*
	Date:
	Signature:

Appendix Five

Subject access request form

Dear Data Protection Officer,

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me and verify the lawfulness of the processing.

Under the GDPR, this information will be provided free of charge, and in most cases, must be provided within 1 month, unless the request is complex and numerous – notification will be given on this eventuality.

Here is the necessary information (To be completed/ supplied by person making request):

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:*

All Subject Access Requests require Head Teacher sign-off.

Name: *Signature:* *Date:*

Appendix Six

Use of Biometric Data – Consent Form.

What Are Biometrics?

Biometrics authentication is the automatic recognition of a living being using suitable body characteristics. By measuring an individual's physical features in an authentication inquiry and comparing this data with stored biometric reference data, the identity of a specific user is determined. There are many different biometric features that can be used for authentication purposes these include finger image, signature, iris, retina, DNA or any other unique characteristic. Once a characteristic has been chosen the next stage in the Biometric process is authentication. A biometric feature is saved on to a database. Once the data has been stored, a new scanning of the biometric feature is taken. If the comparison is positive, access to the appropriate application is granted.

Pupils, parents and colleagues can rest assured that the fingerprint images cannot be used by any other source for identification purposes. The system uses an image of the finger to create a mathematical algorithm and then discards the finger image with only the numbers remaining. These cannot be reinterpreted back into a finger image.

The provider for this system within our school is HC3S. Please find the following information from them:

Use of Biometric Data – Consent Form.

Please sign and date this form to indicate whether or not you consent to your child's biometric information (as described within this letter) being used by the school as part of the biometric recognition system.

Please tick the relevant box(es) below and return this form to school.

I consent to my child's biometric information being using by the school in the ways described above ☐

I do not consent to my child's biometric information being used by the school ☐

If you change your mind at any time, you can let us know by emailing: office@testvalley.hants.sch.uk, calling the school on 01264 810555, or just popping in to the school office. If you have any other questions, please get in touch.

Why are we asking for your consent again?

You may be aware that there are new data protection rules coming in from May 18. To ensure we are meeting the new requirements, we need to re-seek your consent to child's biometric information being used by the school as part of the biometric recognition system.

Pupil Name: ……. Tutor Group: ……...

Parent or carer's signature:……

Date:

Appendix Seven

Consent form for taking and using photos/ videos and social media.

Dear Parent/ Carer,

At Test Valley School, we sometimes take photographs of pupils. We use these photos in the school's prospectus, school's website, social media platforms and on display boards around school.

We would like your consent to take photos of your child and use them in the ways described above. If you're not happy for us to do this, that's no problem – we will accommodate your preferences.

Please tick the relevant box(es) below and return this form to school.

I am happy for the school to take photographs of my child. ☐

I am happy for photos of my child to be used on the school website. ☐

I am happy for photos of my child to be used in the school prospectus. ☐

I am happy for photos of my child to be used in internal displays. ☐

I am happy for photos of my child to be used. ☐

I am **Not** happy for the school to take or use photos of my child. ☐

Consent for Promotional School videos.

We occasionally may consider the use of promotional school videos:

I am happy for my child to be included in promotional school videos ☐

I am **Not** happy for my child to be included in promotional school videos ☐

Consent for Social Media

Occasionally we may consider using social media to promote successes within our school:

I am happy for my child to be included on school social medial platforms ☐

I am **Not** happy for my child to be included on school social media platforms ☐

If you change your mind at any time, you can let us know by emailing: office@testvalley.hants.sch.uk, calling the school on 01264 810555, or just popping into the school office. If you have any other questions, please get in touch.

Why are we asking for your consent again?

To ensure we are GDPR compliant, we need to re-seek your consent to take and use photos and or videos of your child. We really value using images of pupils, to showcase what pupils do in school and show what life at our school is like to others, so we would appreciate you taking the time to give consent again.

Parent or carer's signature: _____ Date:_____

Appendix Eight

Data Privacy Impact Assessments (DPIA) template.
Checklist

Project name:

Brief description of project:

1. What is the project for? What does it seek to achieve?
2. Will the project collect information about individuals e.g. students, parents, staff? If no personal information is collected, a DPIA will not be required.
3. What type of information will it collect? Will it be special category data? e.g. information about an individual's physical or mental health, social care details, details of criminal offences or allegations, or collecting large quantities of personal information? Any of these will raise the level of risk.
4. How will the information be collected? On paper forms? Electronically? Who will have access to this information? How will it be stored and kept secure?

5. How will pupils/staff /parents be made aware of how their personal information is being used? Will a privacy notice be provided? At the end of a paper form? By linking to the school website privacy notice? Does the privacy notice provide sufficient detail about the reasons for collecting the information and who it may be shared with?
6. Do you need consent from the individual to use the information? e.g. because special category data is being collected.
7. Does the project involve the use of new or different technology which could be privacy intrusive e.g. CCTV, monitoring of staff, biometrics, GPS tracking or cloud storage
8. What risks have been identified? What steps have been taken to eliminate or minimise them?
Signature Name (printed) Position Date

Appendix Nine

Pupil Privacy Notice

Introduction

This notice is to help you understand how and why we collect your personal information and what we do with that information. It also explains the decisions that you can make about your own information.

We are giving you this notice because you are mature enough to make decisions about your personal information.

If you have any questions about this notice, please talk to your Year Leader.

What is "personal information"?

Personal information is information that the school holds about you and which identifies you.

This includes information such as your name, date of birth and address as well as things like exam results, medical details and behaviour records. The School may also record your religion or ethnic group. CCTV, photos and video recordings of you are also personal information.

How and why does the school collect and use personal information?

We set out below examples of the different ways in which we use personal information and where this personal information comes from. The primary reason for the School using your personal information is to provide you with an education and to keep you safe.

Admissions forms give us lots of personal information. We get information from you, your parents, your teachers and other pupils. Your old school also gives us information about you so that we can teach and care for you.

Sometimes we get information from your doctors and other professionals where we need this to look after you.

We collect this information to help the school run properly, safely and to let others know what we do here. Here are some examples:

- We need to tell the appropriate teachers if you are allergic to something or might need extra help with some tasks.
- We use CCTV to make sure the school site is safe from uninvited visitors for example (CCTV is not used in private areas such as toilet cubicles or changing rooms).
- We may need to report some of your information to the government. For example, we may need to tell the local authority that you attend the school and let them know if we have any concerns about your welfare.
- We may need information about any court orders or criminal matters which relate to you. This is so that we can safeguard your welfare and wellbeing and the other pupils at the school.
- If you are from another country, then we have to make sure that you have the right to study in the UK. We might have to provide information to UK Visas and Immigration who are part of the government.

- Depending on where you will go when you leave us we may need to provide your information to other schools, colleges and universities or potential employers. For example, if you go on to Sixth Form College we may share information about your exam results and provide references. We may need to pass on information which they need to look after you.

· When you take public examinations (e.g. GCSEs) we will need to share information about you with examination boards. For example, if you require extra time in your exams.

- We may need to share information with the police or our legal advisers if something goes wrong or to help with an inquiry. For example, if one of your classmates is injured at school or if there is a burglary.

- Occasionally we may use consultants, experts and other advisors to assist the school in fulfilling its obligations and to help run the school properly. We might need to share your information with them if this is relevant to their work.

- If you have misbehaved in a serious way, and the police have become involved, we may need to use information about the action taken by the police.

- We will share some information with the Local Education Authority to make sure that we have the insurance cover that we need.

- We may share your academic and your behaviour records with your parents or carer so they can support your schooling.

- We will only share your information with other people and organisations when we have a good reason to do so. In exceptional circumstances we may need to share it more widely than we would normally.

- We will monitor your use of email, the internet and mobile electronic devices e.g. iPhones whilst you are in school. This is to check that you are following are expectations when using this technology and are not putting yourself at risk of harm. If you would like more information about this you can read the IT Rules and Code of Conduct or speak to your Tutor/ Year Leader.

- Where we have previously received permission we may use photographs or videos of you for the school's website or prospectus to show prospective pupils what we do here and to advertise the school.

- Sometimes we use photographs and videos for teaching purposes, for example, to record a Drama or PE lesson.

- If you have concerns about us using photographs or videos of you, please speak to your Year Leader.

- We publish our public exam results, sports fixtures and other news on the website and put articles and photographs in the local news to celebrate what we have been doing.

- We may keep details of your address when you leave so we can send you the details of Test Valley School Alumni.

- Where we have previously received permission we use a Biometric system for the payment of school meals known as “cashless dining”. We do this because the system is secure and it makes the serving of school meals a faster and easier process. Your fingerprint is converted into a secure algorithm which is stored on the school network and is deleted when you leave the school. Your actual fingerprint is not stored and fingerprints cannot be re-created from the secure algorithm.

If you have any concerns about any of the above, please speak to your Year Leader.

Our legal grounds for using your information

This section contains information about the legal basis that we are relying on when handling your information.

1. "Legitimate interests"

This means that the processing is necessary for to meet its legitimate interests in providing you with an education. The school relies on legitimate interests for most of the ways in which it uses your information.

Specifically, the school has a legitimate interest in:

- Providing you with an education.
- Safeguarding and promoting your welfare and the welfare of other children.
- Promoting the objects and interests of the school. This includes fundraising e.g. if we want to raise money to fund special projects.
- Facilitating the efficient operation of the school.
- Ensuring that all relevant legal obligations of the school are complied with.

In addition, your personal information may be processed for the legitimate interests of others. For example, we may use information about you when investigating a complaint made by one of your fellow pupils.

2. "Legal obligation"

Where the School needs to use your information in order to comply with a legal obligation, for example to report a concern about your wellbeing to Children's Services. We may also have to disclose your information to third parties such as the courts, the local authority or the police where legally obliged to do so.

3. "Vital interests"

For example, to prevent someone from being seriously harmed or killed or to protect the vital interests of any person where that person cannot give consent, for example, if they are seriously hurt and are unconscious.

4. "Public interest"

Test Valley School considers that it is acting in the public interest when providing education.

Test Valley School must also comply with an additional condition where it processes special categories of personal information. These special categories include: personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic information, biometric information, health information, and information about sex life or orientation.

5. "Substantial public interest"

The processing is necessary for reasons of substantial public interest.

6. "Legal claims"

The processing is necessary for the establishment, exercise or defence of legal claims. This allows us to share information with our Local Education Authority, legal advisors and insurers.

7. "Medical purposes"

This includes medical treatment and the management of healthcare services.

We may ask for your consent to use your information in certain ways. If we ask for your consent to use your personal information you can take back this consent at any time. Any use of your information before you withdraw your consent remains valid. Please speak to your Head of Year if you would like to withdraw any consent given.

Sending information to other countries

We may send your information to other countries where:

- We store information on computer servers based overseas; or
- We communicate with you or your parents when you are overseas (for example, during the summer holidays if you holiday in a different country).

For how long do we keep your information?

We keep your information for as long as we need to in order to educate and look after you and until you are at least 22 years old in order to comply with our legal obligations.

What decisions can you make about your information?

Your rights are as follows:

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

Further information and guidance

This notice is to explain how we look after your personal information. Your Head of Year can answer any questions which you might have.

Please speak to your Head of Year if:

- You object to us using your information for marketing purposes e.g. to send you information about school events. We will stop using your information for marketing purposes if you tell us not to; or
- You would like us to update the information we hold about you; or
- You would prefer that certain information is kept confidential.

Test Valley School is registered as the Data Controller with the Information Commissioners Office.

The Data Protection Officer and is the person responsible at our school for managing how we look after personal information and deciding how it is shared. If you have any questions you can ask your Head of Year about how it works in our school.

Alternatively, you can ask your parents to speak to us on your behalf if you prefer.

Appendix Ten

Privacy Notice – General Data Protection Regulation 2018

Test Valley School is the data controller for the purposes of the General Data Protection Regulation. We collect information from you and may receive information about you from your previous school, Hampshire County Council and the Learning Records Service. We hold this personal data and use/share it to:

- Support pupils' teaching and learning;
- Monitor and report on pupil progress;
- Provide appropriate pastoral care;
- Contribute to improving pupil health and reducing inequalities
- Undertake statistical forecasting and planning; and
- Assess how well Test Valley School is performing.

This information includes parental contact details, national curriculum assessment results, attendance information modes of travel and personal characteristics such as ethnic group, any special educational needs and relevant medical information.

The school is protected by CCTV in all public spaces but not in toilet cubicles or changing areas.

If we have received your permission, then we may store and share photographs or video for use in our news stories, on our website or prospectus.

If we have received permission, then we use pupil biometric data to support our cashless catering system.

If pupils are enrolling for post 14 qualifications, then the school will be provided with a pupil unique learner number (ULN) by the Learning Records Service and the school may also obtain from them details of any learning or qualifications that have been undertaken.

We collect and use this information in order to meet the school's legitimate interest in providing an education, safeguarding pupil welfare and in ensuring that the school complies with its legal obligations. Whilst most of the information provided is mandatory, we rely on consent to use some data including photographs, video and biometric data.

We will not give information about pupils, parents or guardians to anyone outside the school without their consent unless the law allows us to.

We are required by law to pass some information about pupils to the Local Authority and the Department for Education (DfE). Once pupils are aged 13 or over, we are required by law to pass on certain information to the providers of youth support services in your area. This is the local authority support service for young people aged 13 to 19 in England. We must provide the name and address of pupils and their parents (including date of birth) and any further information relevant to the support services' role.

However, until pupils are aged 16 or older, then parents / guardians can ask that no information beyond pupil name, address and date of birth (and name and address) be passed on to the youth services provider. This right transfers to the pupil on their 16th birthday. Please inform the school office if pupils or their parents wish to opt-out of this arrangement.

For more information about young peoples' services, please go to the National Careers Service page at https://nationalcareersservice.direct.gov.uk/aboutus/Pages/default.aspx.

For more information about the Youth Support Services in Hampshire please go to http://www3.hants.gov.uk/yourfuture/yourfuture-aboutus.htm.

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

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

For Hampshire County Council:
The County Council has their own privacy notice, which can be accessed via the following link:
http://www3.hants.gov.uk/hcc_csd_privacy_notice_-_generic__sept_2014_-2.doc

To see how your information is used by the LA:
http://www3.hants.gov.uk/education/schools/schoolsdataprotection.htm#section242880-3

For the DfE:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

- Data Protection Team
  Children's Services
  Elizabeth II Court (North)
  The Castle
  WINCHESTER
  SO23 8UQ
  Website: http://www3.hants.gov.uk/learning
  email: childrens.services.dp@hants.gov.uk
  Telephone: 01962 845320

- Public Communications Unit
  Department for Education
  Sanctuary Buildings
  Great Smith Street
  London
  SW1P 3BT
  Website: https://www.gov.uk/government/organisations/department-for-education
  email: http://www.education.gov.uk/help/contactus
  Telephone: 0370 000 2288

Test Valley School is registered as the Data Controller with the Information Commissioners Office (Registration reference: ZA336960). For more information please see the Pupil Privacy Notice. If you have any questions, please contact the school's Data Protection Officer, via the school office, or office@testvalley.hants.sch.uk.

Appendix Eleven

Colleague Privacy Notice

Introduction

This notice is to help you understand how and why we collect your personal information and what we do with that information. It also explains the decisions that you can make about your own information.

What is "personal information"?

Personal information is data that the school holds about you and which identifies you.

This includes information such as your name, date of birth and address as well as things like your recruitment information, qualifications & biometrics. The school may also record your religion or ethnic group. CCTV, photos and video recordings of you are also personal information which the school holds.

How and why does the School collect and use personal information?

We set out below examples of the different ways in which we use personal information and where this personal information comes from. The primary reason for using your personal information is as your employer. Legally we are required to keep certain documentation.

Application forms give us lots of personal information. We get this information from you when you apply to work here at Test Valley School. Legally we require this information so that we can ensure we abide by right to work regulations and also to ensure all relevant safeguarding checks are completed.

We collect this information to help the school run properly, safely and to let others know what we do here. Here are some examples:

- We use CCTV to make sure the school site is safe. CCTV is not used in private areas such as toilet cubicles or changing rooms.
- We may need to report some of your information to the government. For example, we may need to tell the local authority our staff numbers and the subject areas our staff work within to ensure we are following all relevant guidelines and legislation.
- We may need to share information with the police or our legal advisers if something goes wrong or to help with an inquiry. For example, if one of your colleagues is injured at school or if there is a burglary.
- Occasionally we may use consultants, experts and other advisors to assist the school in fulfilling its obligations and to help run the school properly. We might need to share your information with them if this is relevant to their work.
- We may share some information with the Local Education Authority to make sure that we have the insurance cover that we need.
- We will only share your information with other people and organisations when we have a good reason to do so. In exceptional circumstances we may need to share it more widely than we would normally.
- We will monitor your use of email and the internet whilst you are in school. This is to check that the IT Rules and Code of Conduct are being adhered to.
- Where we have previously received permission we may use photographs or videos of you for the school's website or prospectus to show prospective pupils what we do here and to advertise the school.

- If you have concerns about us using photographs or videos of you, please speak to your Line Manager.

If you have any concerns about any of the above, please speak to your Line Manager.

Our legal grounds for using your information

This section contains information about the legal basis that we are relying on when handling your information.

1. Legitimate interests

This means that the processing is necessary for legitimate interests except where the processing is unfair to you. The school relies on legitimate interests for most of the ways in which it uses your information.

Specifically, the school has a legitimate interest in:

- Being your employer.
- Safeguarding and promoting your welfare whilst in school.
- Promoting the objects and interests of the school. This includes fundraising e.g. if we want to raise money to fund special projects.
- Facilitating the efficient operation of the school.
- Ensuring that all relevant legal obligations of the school are complied with.

In addition, your personal information may be processed for the legitimate interests of others. For example, we may use information about you when investigating a complaint.

2. Legal obligation

Where the School needs to use your information in order to comply with a legal obligation, for example if an incident occurs. We may also have to disclose your information to third parties such as the courts, the local authority or the police where legally obliged to do so.

3. Vital interests

For example, to prevent someone from being seriously harmed or killed or to protect the vital interests of any person where that person cannot give consent, for example, if they are seriously hurt and are unconscious.

4. Public interest

Test Valley School considers that it is acting in the public interest when providing education.

Test Valley School must also comply with an additional condition where it processes special categories of personal information. These special categories include: personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic information, biometric information, health information, and information about sex life or orientation.

5. Substantial public interest

The processing is necessary for reasons of substantial public interest.

6. Legal claims

The processing is necessary for the establishment, exercise or defence of legal claims. This allows us to share information with our Local Education Authority, legal advisors and insurers.

7. Medical purposes

This includes medical treatment and the management of healthcare services.

We may ask for your consent to use your information in certain ways. If we ask for your consent to use your personal information you can take back this consent at any time. Any use of your information before you withdraw your consent remains valid. Please speak to your Line Manager if you would like to withdraw any consent given.

Sending information to other countries

We may send your information to other countries where:

- We store information on computer servers based overseas; or
- We communicate with you when you are overseas (for example, during the summer holidays if you holiday in a different country).

For how long do we keep your information?

We keep your information for as long as your employment lasts +7 years in order to comply with our legal obligations.

What decisions can you make about your information?

Your rights are as follows:

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

The Data Protection Officer can give you more information about your data protection rights.

Further information and guidance

This notice is to explain how to store and guard your personal information. The Senior IT lead is the Data Protection Officer and can answer any questions which you might have.

Please speak to the Data Protection Officer if:

- You object to us using your information for marketing purposes e.g. to send you information about school events. We will stop using your information for marketing purposes if you tell us not to.
- Or you would like us to update the information we hold about you.
- Or if you would prefer that certain information is kept confidential.
-

Test Valley School is registered as the Data Controller with the Information Commissioners Office (Registration reference: Z6454920).

If you consider that we have not acted properly when using your personal information, you can contact the Information Commissioner's Office: www.ico.org.uk.

Appendix Twelve

Personal Data breach procedure.

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged later by the ICO or an individual affected by the breach. Documented decisions are stored on the school's backed up Data storage network GDPR area. The nominated Governor Data Protection Link along with the Headteacher will be notified.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours, using the templated Data Breach Reporting Form found at Appendix Thirteen. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts, cause and effect
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the school's backed up Data storage network GDPR area. The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

The following are our relevant actions we will take for different types of risky or sensitive personal data processed by your school.

Sensitive information being disclosed via email (including safeguarding records):

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask our onsite IT support to attempt to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked, and parents' financial details stolen
- Loss of individual Medical care plans
- Loss of Personal folder/ information.

Appendix Thirteen - Data Breach Reporting Form.

Information Commissioner's Office

Report a personal data breach

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. **Please do not include any of the personal data involved in the breach when completing this form**. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

About your report

Please answer the following questions, to help us handle your report efficiently and to better understand our customers.

If you have already spoken to a member of ICO staff about this breach, please give their name:

Report type

- Initial report – report complete
- Follow-up report – report complete
- Initial report – additional information to follow
- Follow-up report – additional information to follow

(Follow-up reports only) ICO case reference:

Reason for report – after consulting the guidance

- I consider the incident meets the threshold to report
- I do not consider the incident meets the threshold to report, however I want you to be aware
- I am unclear whether the incident meets the threshold to report

Size of organisation

- Fewer than 250 staff
- 250 staff or more

Is this the first time you have contacted us about a breach since the GDPR came into force?

- Yes
- No
- Unknown

About the breach

Please describe what happened

Please describe how the incident occurred

How did the organisation discover the breach?

What preventative measures did you have in place?

Was the breach caused by a cyber incident?

Yes

No

Don't know

When did the breach happen?

Date: Time:

When did you discover the breach?

Date: Time:

Categories of personal data included in the breach (tick all that apply)

☐ Data revealing racial or ethnic origin

☐ Political opinions

☐ Religious or philosophical beliefs

☐ Trade union membership

☐ Sex life data

☐ Sexual orientation data

☐ Gender reassignment data

☐ Health data

☐ Basic personal identifiers, eg name, contact details

☐ Identification data, eg usernames, passwords

☐ Economic and financial data, eg credit card numbers, bank details

☐ Official documents, eg driving licences

☐ Location data, eg coordinates

☐ Genetic or biometric data

☐ Criminal convictions, offences

☐ Other (please give details below)

Please give additional details to help us understand the nature of the personal data included in the breach:

Number of personal data records concerned?

How many data subjects could be affected?

(Cyber incidents only) If the number of data subjects affected is not known, estimate the maximum possible number that could be affected/total customer base

Categories of data subjects affected (tick all that apply)

☐ Employees

☐ Users

☐ Subscribers

☐ Students

☐ Customers or prospective customers

☐ Patients

☐ Children

☐ Vulnerable adults

☐ Other (please give details below)

Describe any detriment to individuals that has arisen so far, or any detriment you anticipate may arise in the future

Is the personal data breach likely to result in a high risk to data subjects?

Yes

No

Not yet known

Please give details

(Cyber incidents only) Recovery time

We have successfully recovered from the incident with all personal data now at the same state it was shortly prior to the incident

We have determined that we are able to restore all personal data to the same state it was shortly prior to the incident and are in the process of doing this

We have determined that we are unable to restore the personal data to the same state it was at shortly prior to the incident, ie backups failed, no current backup, backup encrypted etc

We are not yet able to determine if personal data can be restored to the same state it was shortly prior to the incident

Had the staff member involved in this breach received data protection training in the last two years?

Yes

No

Don't know

Please describe the data protection training you provide, including an outline of training content and frequency

(Initial reports only) If there has been a delay in reporting this breach, please explain why

Taking action

Have you taken action to contain the breach or limit its impact? Please describe these remedial actions

Please outline any steps you are taking to prevent a recurrence, and when you expect they will be completed

Describe any further action you have taken, or propose to take, as a result of the breach

Have you told data subjects about the breach?

Yes – we have determined it is likely there is a high risk to data subjects so we have communicated this breach to data subjects

Yes – we have determined that it is unlikely there is a high risk to data subjects, however decided to tell them anyway

No – but we are planning to because we have determined it is likely there is a high risk to data subjects

No – we determined the incident did not meet the threshold for communicating it to data subjects

Have you told, or are you planning to tell any other organisations about the breach?

Yes

No

Don't know

If you answered yes, please specify

Are you a member of a UK GDPR Code of Conduct or Certification Scheme, as approved and published on the ICO website?

Yes

No

If yes:

Please confirm the Code/Scheme name

Are the Code or Scheme's requirements relevant to the breach that has occurred?

Yes

No

Have you informed the relevant Monitoring Body or Certification Body?

Yes

No

Suspicious websites

If the breach relates to a suspicious website, you can report the website to the National Cyber Security Centre (NCSC). By reporting, you can help stop cyber criminals and protect others online.

The ICO won't see the details of your report to NCSC, so you should make sure you tell us everything we need to know on this form.

Report a suspicious website - NCSC.GOV.UK

About you

Organisation (data controller) name

Registration number

If not registered, please give exemption reason

Business sector

Registered organisation address

Person making this report

In case we need to contact you about this report

Name:

Email:

Phone:

Sending this form

Initial report

If this is your initial report, please send your completed form to icocasework@ico.org.uk, with 'Personal data breach notification' in the subject field.

Follow up report

If this is a follow up report, please *reply to the email we sent you*, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case).

OR, send by post to:

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

Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

You should read our guidance to determine what steps you should take.

Based on the information you have provided, we will contact you within seven calendar days to provide information about our next steps. If this is your initial report, we'll give you a case reference number.

If your correspondence relates to an existing case, we'll add it to your case for your case officer to consider.

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

For information about what we do with personal data see our privacy notice.