DATA PROTECTION POLICY
May 2018

Approved: 15th May 2018, Operations & Resources' Committee

Review Date: May 2019

Links with other Policies

The Tapscott Learning Trust Data Protection Policy is written in line with General Data Protection Regulations (GDPR) of 2018. When agreeing or reviewing the policy, links should be made with other relevant policies and guidelines, including Freedom of Information Act, Safeguarding Policy, Whistleblowing Policy, Personal Safety and Security Policy , Retention and Destruction Policy (IRMS) and Online Policy with E-Safety.

Contents

1. Purpose

The purpose of this policy is to ensure that the schools within The Tapscott Learning Trust (hereon called the "Trust " or "TTLT") are committed to compliance with all the relevant data protection laws in respect of personal data, and to protecting the "rights and freedoms" of individuals whose information the schools collects about staff, pupils, parents, governors, visitors and other individuals, are stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

To that end, schools have developed, implemented, maintains and continuously improves a documented personal information management system (PIMS) in each school. The scope of PIMS takes into account the school structure, management responsibility, jurisdiction and geography. Each school's objectives for PIMS is that it should enable the school to meet its own requirements for the management of personal information; that it should support school objectives and obligations; that it should impose controls in line with the schools' acceptable level of risk; that it should ensure that the school meets applicable statutory, regulatory, contractual and / or professional duties; and that it should protect the interests of individuals and other key stakeholders.

In meeting PIMS this policy applies to all personal data of natural persons, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR, alongside the guides to GDPR, including *Preparing for the General Data Protection Regulation (GDPR) 12 Steps to Take Now*, and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

Due regard to is given to the following legislations: *The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations (2004)* and *The School Standards and Framework Act (1998)*.

In addition, this policy complies with our funding agreement and articles of association.

3. Objectives

The school is committed to complying with data protection legislation and good practice including:

- processing personal information only where this is strictly necessary for legitimate organisational purposes;
- collecting only the minimum personal information required for these purposes and not processing excessive personal information;
- providing clear information to individuals about how their personal information will be used and by whom;
- only processing relevant and adequate personal information;

- processing personal information fairly and lawfully;
- maintaining an inventory of the categories of personal information processed by the school;
- keeping personal information accurate and, where necessary, up to date;
- retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes;
- respecting individuals' rights in relation to their personal information, including their right of subject access;
- keeping all personal information secure;
- only transferring personal information outside the EU in circumstances where it can be adequately protected;
- the application of the various exemptions allowable by data protection legislation;
- developing and implementing a PIMS to enable the policy to be implemented
- where appropriate, identifying internal and external stakeholders and the degree to which these stakeholders are involved in the governance of the school's PIMS;
- the identification of employees with specific responsibility and accountability for the PIMS; and
- carry out an annual audit of General Data Protection.

4. Explaining the Language Around Data Protection

Term	Description	Example
Automated decision making / profiling	This is when machines / software apply rules to data and determine something about someone based on purely applying those rules. Typically it is the significance of the decision which drives the caution and concern here. Read further information.	"Anyone recorded as attendance >99% will get a voucher for X"
Child	The GDPR defines a child as anyone under the age of 16 years old. The processing of personal data of a child under 13 (under UK law) years of age is only lawful if parental or custodian consent has been obtained.	
Data controller	The organisation who (either alone or in common with other people) determine the purpose for which, and the manner in which data are processed.	A school is often the data controller, sometimes a joint controller with the Trust.
Data breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the	Sending a list of pupil names, attainment marks and dates of births to the wrong school.

	result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.	
Data item	A single piece of information about a data subject.	“Ethnicity = white British” “Attendance = 97%”
Data item group	A group of data items that are typically captured about the same activity or business process in school. These are also sometimes called data elements or data scope within the data community/sharing agreements schools have with suppliers.	Behaviour management or catering.
Data processor	A person or organisation that process data on behalf of and on the orders of a data controller.	A catering supplier the school uses.
Data Protection Impact Assessment (DPIA)	This is a process to consider the implications of some change you are introducing on the privacy of individuals. Assessing privacy at the outset helps you plan consultation / awareness / consent type options from the outset. “Privacy by design” is a term that is used in this space.	For example, you would undertake one of these if introducing a new system to use fingerprinting within catering provision.
Data retention	How long you will hold information for to do the processing job you need it for. At the end of a data retention period, processes should be in place to ensure it is properly disposed of.	An example: “We keep parent’s phone numbers until 1 month after they leave the school in case of any issues that need resolving (for example, payment or repayment of lunch money) and then it is deleted.”
Data subject	The person that the data relates to.	John Smith the pupil. Jane Smith the teacher.
Data subject consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.	Signing of a document giving explicit consent for something specific.

Filing system	Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.	
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.	
Privacy notice / Fair processing	This is a document that explains to the people you have data about ("data subjects") the data items you hold, what they are used for, who it is passed onto and why, and what rights they have.	DfE publish model privacy notices.
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.	
Profiling	This is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence	

	of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.	
Special category data	These are highly sensitive pieces of information about people. They are important because under GDPR they are afforded extra protection in terms of the reasons you need to have to access and process that information. In education, it would also be best practice to treat things like FSM, SEN, and CIN/CLA status as special category data.	Tightly defined as data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, health, trade-union membership, and health or sex life. Data relating to criminal offences is also afforded similar special protection.
Subject Access Request (SAR)	This is where a person (data subject), requests access to the information you hold about them. Timescales for responding, as well as reasons why you must comply or may refuse, as set out in law. A Subject Access Request is often used to describe “tell me all my data you hold”.	“I want to know the attendance data you hold about my son”
System	A piece of software, computer package or manually managed asset that supports the administration of one or more areas of school life.	Capita SIMS, ParentPay.
System group	An umbrella term to describe the areas of school administration where systems that contain personal level data typically reside.	Core MIS, payments, curriculum tools.
Territorial scope	The GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour to data subjects who are resident in the EU.	
Third party	A natural or legal person, public authority, agency or body other than the data subject, controller, processor	

	and persons who, under the direct authority of the controller or processor, are authorised to process personal data.	

5. Roles and responsibilities

5.1 The Data Controller

Every school within the Trust and the Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore are data controllers and data processors under GDPR.

Each of the schools is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5.2 Trustees and Local Advisory Boards (LABs)

The Trustees and Governors have overall responsibility for ensuring that all schools within the Trust comply with all relevant data protection obligations.

5.3 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 periodic reports and updates to the relevant LABs and committees of their activities directly and, where relevant, report their advice and recommendations on school data protection issues.

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

Full details of the DPO's responsibilities are set out in their job description. Suitable training has been gained in fulfilling this role as part of continuing professional development within each school's professional training programme.

The Trust's GDPR working party is made of the following DPOs, including Rebecca Cheetham Nursery and Children's Centre who are working in partnership with TTLT:

Rohan Allen, Head Teacher, Rebecca Cheetam Nursery

Shella Lawrenson, Head Teacher, Ranelagh Primary School

Swasthi Mahabeer, Teacher at Curwen Primary School and Trust Policy Lead

Femi Otukoya, Finance Director, TTLT

Shazidur Rahman, School Business Manager, Kensington Primary School

To avoid conflict of interest TTLT shares the DPO function between a group of schools and shares expertise by being the DPOs for each other's school.

5.4 Chief Executive Officer (CEO)

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

5.5 Head Teachers / Head of School

The Head Teacher / Head of School and all those in managerial or supervisory roles throughout the school are responsible for developing and encouraging good information handling practices within the school; responsibilities are set out in individual job descriptions.

The Head Teacher / Head of School, a member of the senior management team, is accountable to the CEO for the management of personal information within their school and for ensuring that compliance with data protection legislation and good practice can be demonstrated.

This accountability includes:

1. Development and implementation of the PIMS as required by this policy
2. Security and risk management in relation to compliance with the policy

- The Head Teacher considers to be suitably qualified and experienced, has been appointed to take responsibility for the school's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that the school complies with the GDPR, as do managers in respect of data processing that takes place within their area of responsibility.

The DPO have specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees / Staff seeking clarification on any aspect of data protection compliance before contacting the Head Teacher.

5.6 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting 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 they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they 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

- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

Compliance with data protection legislation is the responsibility of all members of the school who process personal information.

The school's continuing professional development sets out specific training and awareness requirements in relation to all staff.

Members of the school are responsible for ensuring that any personal data supplied by them, and that is about them, to the school is accurate and up-to-date.

6. 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:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 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**

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 bug club, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.2 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 in order 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 Information and Records Management Society's toolkit for schools (IRMS).

A systematic destruction of documents is carried out at the end of the academic year in line with IRMS.

8. 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 which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement (see Appendix A) 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 European Economic Area, we will do so in accordance with data protection law.

9. Subject Access Requests and Other Rights of Individuals

9.1 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

Subject access requests (see Appendix B) must be submitted in writing, either by letter, email or fax to the DPO. They should include:

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

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

9.2 Children and Subject Access Requests

Children below the age of 13 are generally not 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 schools may 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. From the age of 13 children have a right to access their data.

9.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- 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 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 excessive, we may refuse to act on it, or charge a reasonable fee which takes into account 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.

9.4 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 7), 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 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.

10. Parental Requests to See the Educational Record

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

Use the subject access request form to submit your request.

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 School Business Manager.

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 parent / carer and pupil.

Upon admission to schools within TTLT, 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 parent / carer and pupil.

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.

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:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert 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 privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices (see Appendices C [Privacy Notice – The Trust as an Educational Setting], D [Privacy Notice for Pupils], E [Privacy Notice for Parents / Carers], F [Privacy Notice for Staff])

- 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 servers 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
- Passwords 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 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
- 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 8)

15. Disposal of Records

Personal data that is no longer needed will be disposed of securely in line with IRMS.

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 procedure set out in Appendix G with a Breach Incident Form (See Appendix H).

When appropriate, we will report the data breach to the ICO within 72 hours. 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 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.

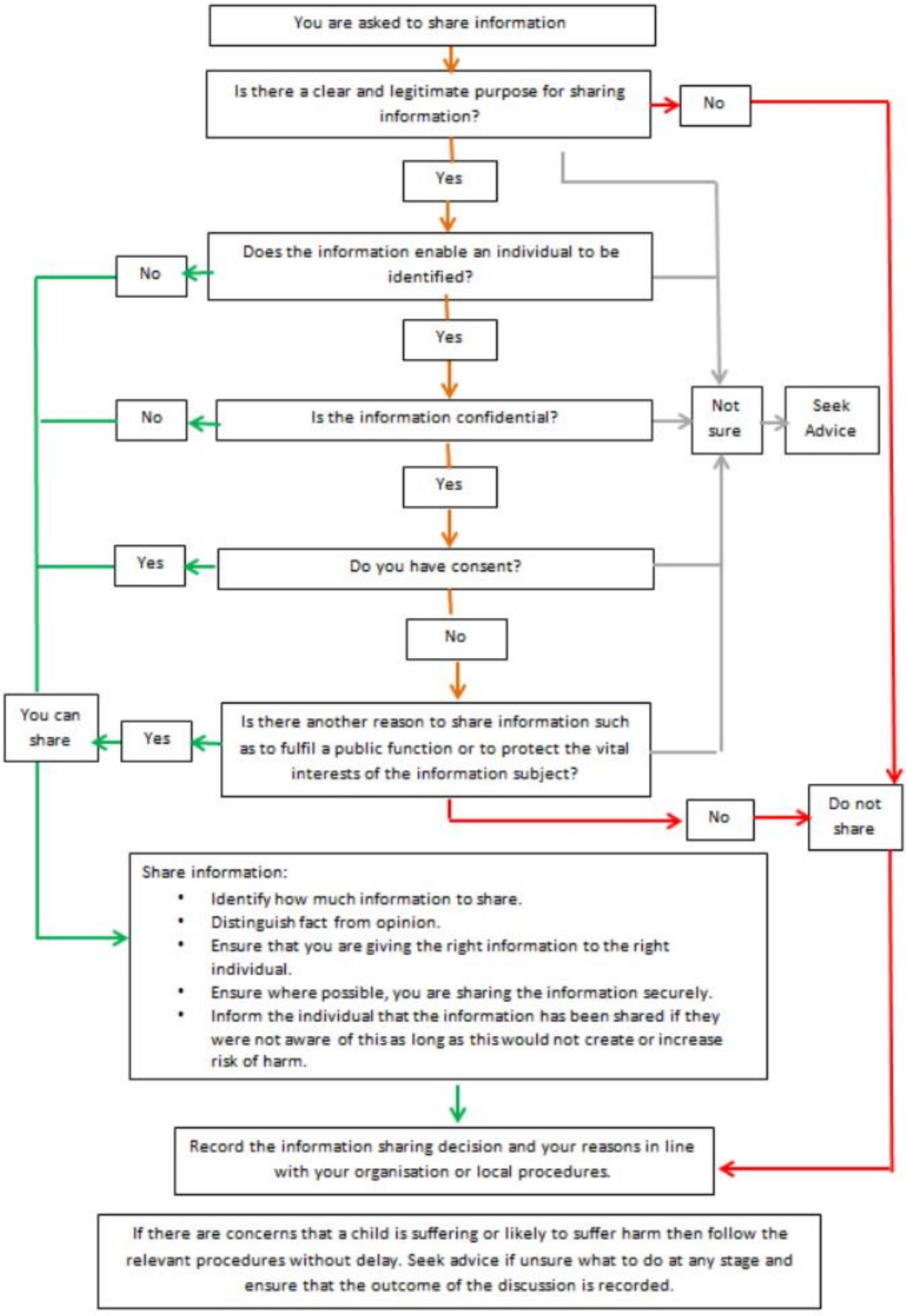
18. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **annually** and shared with the full governing board.

Appendix A: Data Sharing Agreement

The Department for Education (DfE) produced guidance on information sharing for practitioners providing safeguarding services. It was written for the Data Protection Act, but it should be used until more up-to-date guidance is provided for the upcoming GDPR.



Appendix B: Subject Access Requests

On the school letterhead

Re: Subject Access Request

Dear Head Teacher / Head of School,

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.
Here is the necessary information:

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:* • *Your personnel file* • *Your child's medical records* • *Your child's behavior record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

If you need any more information from me, please let me know as soon as possible. Please bear in mind that under the GDPR you cannot charge a fee to provide this information, and in most cases, must supply me with the information within 1 month.
If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,

Your name_____

Signature_____

Appendix C: Privacy Notice – The Trust as an Educational Setting

Privacy Notice – The Trust as an Educational Setting
The Data Protection Act 1998: How we use pupil information

Why do we collect and use pupil information?

We collect and use pupil information under the Trust under the lawful basis for collecting and using pupil information for general purposes under Article 6 and Article 9 of the GDPR May 2018 Working Party, where data processed is special category data.

We use the pupil data:

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

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

- Personal information (such as name, unique pupil number and address);
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility);
- Attendance information (such as sessions attended, number of absences and absence reasons);
- Attainment, Examination & Assessment information to support pupil learning;
- Medical information provided by parents/carers and guardians;
- Special Educational Needs and Referral Information;
- Behavioural Information, including exclusions;
- Court of Protection/Safeguarding information;
- Photographic images in our schools, on school literature, websites or media;

Collecting pupil information

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

Storing pupil data

We hold pupil data from the point that an application is made through our Schools or the Local Authority. These records are retained until the child is 25 years of age, as well as

being transferred to the relevant secondary school and held until the child is 25 years of age.

Who do we share pupil information with?

We routinely share pupil information with:

- Members and Trustees of Consortium in the support of pupil learning
- Trust staff in the support of pupil learning
- The school's Local Governing Body
- Consultants engaged by the Trust to support pupil learning
- Staff of other Trust schools in the support of pupil learning
- Staff of Partnership schools in the support of pupil learning
- Cloud based educational programmes to support pupil learning and communication
- Parents & Carers of our schools
- School Nursing & Dental Services
- External agencies; health, SEND, child protection, welfare and safeguarding services
- Local media publications
- Schools that the pupil's attend after leaving us
- The school's local authority
- The Department for Education (DfE)

Why we share pupil information

We do not share information about our pupils with anyone without consent, unless the law and our policies allow us to do so. We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

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

Data collection requirements:

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

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

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

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data.

Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;
- the level and sensitivity of data requested, and
- the arrangements in place to store and handle the data;

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

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

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:

https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the Data Protection Officer for the Trust who is Shazidur Rahman:

Shazidur.rahman@kensington.ttlt.academy

You also have the right to:

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

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

Contact:

If you would like to discuss anything in this privacy notice, please contact the Data Protection Officer for the Trust, who is Shazidur Rahman at:

Shazidur.rahman@kensington.ttlt.academy

Appendix D: Privacy Notice for Pupils

Privacy Notice for Pupils
Summer 2018

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This privacy notice explains how we collect, store and use personal data about you.
We, The Tapscott Learning Trust (hereon called the "Trust" or "TTLT") and its schools are the 'data controllers' for the purposes of data protection law.

Our data protection officer can be found on the TTLT or school's website.

The personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.

This information includes:

- Your contact details
- Your test results
- Your attendance records
- Your characteristics, like your ethnic background or any special educational needs
- Any medical conditions you have
- Details of any behaviour issues or exclusions
- Photographs
- CCTV images

Why we use this data

We use this data to help run the school, including to:

- Get in touch with you and your parents when we need to
- Check how you're doing in exams and work out whether you or your teachers need any extra help
- Track how well the school as a whole is performing
- Look after your wellbeing

Our legal basis for using this data

We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- You, or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interest)

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.

Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

Collecting this information

While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.

We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How we store this data

We will keep personal information about you while you are a pupil at our school. We may also keep it after you have left the school, where we are required to by law.

We use the Information and Records Management Society's toolkit for schools which sets out how long we must keep information about pupils.

Data sharing

We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- Our local authority – to meet our legal duties to share certain information with it, such as concerns about pupils' safety and exclusions
- The Department for Education (a government department)
- Your family and representatives
- Educators and examining bodies
- Our regulator, e.g. OfSTED

- Suppliers and service providers – so that they can provide the services we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Police forces, courts, tribunals
- Professional bodies

National Pupil Database

We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.

Some of this information is then stored in the National Pupil Database, which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data. You can find more information about this on the Department for Education's webpage on how it collects and shares research data.

You can also contact the Department for Education if you have any questions about the database.

Transferring data internationally

Where we share data with an organisation that is based outside the European Economic Area, we will protect your data by following data protection law.

Your rights

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 below the age of 12 are generally not 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 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.

How to access personal information we hold about you
You can find out if we hold any personal information about you, and how we use it, by making a **'subject access request'**, as long as we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.

If you want to make a request please contact our data protection officer.

Your other rights over your data

You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don't want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don't want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.

You can make a complaint at any time by contacting our data protection officer.
You can also complain to the Information Commissioner's Office in one of the following ways:

- 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 the relevant data protection officer at your school.

Appendix E: Privacy Notice for Parents / Carers

Privacy notice for Parents / Carers
Summer 2018

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, [school name and address], are the 'data controller' for the purposes of data protection law.

Our data protection officer can be found on the TTLT or school's website.

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
- CCTV images captured in school

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
- Administer admissions waiting lists
- 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. The Information and Records Management Society's toolkit for schoolssets out how long we keep information about pupils.

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
- The pupil's family and representatives

- Educators and examining bodies
- Our regulator [specify as appropriate, e.g. Ofsted, Independent Schools Inspectorate]
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Police forces, courts, tribunals
- Professional bodies

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.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

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 right to access to their child's **educational record**. To request access, please contact the DPO.

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 us in the first instance.

To make a complaint, please contact our data protection officer.

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 the relevant **data protection officer**.

Appendix F: Privacy Notice for Staff

Privacy Notice for Staff
Summer 2018

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, [school name and address], are the 'data controller' for the purposes of data protection law.

Our data protection officers are:

Rohan Allen

Shella Lawrenson

Swasthi Mahabeer

Femi Otukoya

Shazidur Rahman

To avoid conflict of interest TTLT shares the DPO function between a group of schools and shares expertise by being the DPOs for each other's school.
.

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 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 licence
- Photographs
- CCTV footage
- 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 ethnicity and disability 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 when:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)
- We have legitimate interests in processing the data – for example, where:
    - [If you use this basis at all, set out the situations here]

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

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.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with to the Information and Records Management Society's toolkit for schools.

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 [maintained schools only] information about head teacher performance and staff dismissals
- The Department for Education
- Your family or representatives
- Educators and examining bodies
- Our regulator [specify as appropriate e.g. OfSTED, Independent Schools Inspectorate]
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Trade unions and associations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

Transferring data internationally

If we are required to 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 us in the first instance.

To make a complaint, please contact our data protection officer.

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 the respective **data protection officer**:

Appendix G: 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 incident and fill in the Breach Incident Form (see Appendix H)

- 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 review incident with another Trust DPO and agree severity and any remedial actions and determine the next required actions. They will consider whether personal data has been accidentally or unlawfully breached. A breach can be:
    - the disclosure of confidential data to unauthorised individuals
    - the loss or theft of portable devices or equipment containing identifiable personal, confidential or sensitive data e.g. PCs, USBs, mobile phones, laptops, disks etc.
    - the loss or theft of paper records
    - inappropriate access controls allowing unauthorised use of information
    - a suspected breach of the school's IT security and acceptable use policy
    - attempts to gain unauthorised access to computer systems, e.g. hacking
    - records altered or deleted without authorisation from the data 'owner'
    - viruses or other security attacks on IT equipment systems or networks
    - breaches of physical security, for example forcing of doors or windows into a secure room or filing cabinet containing confidential information
    - confidential information left unlocked in accessible areas
    - insecure disposal of confidential paper waste
    - leaving IT equipment unattended when logged in to a user account without locking the screen to stop others accessing information
    - the publication of confidential data on the internet in error and accidental disclosure of passwords
    - misdirected emails or faxes containing identifiable personal, confidential or sensitive data

- Both DPOs will:
    - alert the CEO / Head Teacher / Head of School and the Chair of Governors, as necessary
    - 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

- Both DPOs will document the decision (either way); in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored

- Where the ICO must be notified, the DPOs will do this via the 'report a breach' page of the ICO website within 72 hours. 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 DPOs 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 DPOs will submit the remaining information as soon as possible

- Both DPOs 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 DPOs 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 DPOs 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 DPOs will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - 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 documented within the Breach Incident Form, as per the Health and Safety Policy.

- The DPO and CEO / Head Teacher / Head of School 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.

Examples of actions (for different types of risky or sensitive personal data) are:

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 the ICT department 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 that you might want to consider 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

Appendix H: Personal data breach procedure

Breach Incident Reporting Form

School Details

Name of School	
Address	
Name of Data Protection Officer	

Notice of Personal Data Breach

Date of breach	
Description of Breach	
Impact of Breach	
Number of data subjects affected	
Personal data affected	
Number of personal data records affected	
Likely consequences of the breach	
Remedial action taken	
Date of remediation	
Report to ICO	

SIGNED	
NAME AND TITLE	