Data Protection Policy

Approval and Authorisation

	Name	Role	Date
Author	Gareth Kitchen	Information Governance Manager	17/12/2019
Reviewers	Annamaria Cooper	Head of Technology Governance	17/12/2019

Approvers	Name	Role	Date
	Aidan Gray	Group IT Director	17/12/2019

Change History

Version	Author	Revision Details	Date
v.0.1	Gareth Kitchen		
v.1.0	Gareth Kitchen	Draft signed off.	
v.1.1	Gareth Kitchen	Updates to reflect Tes wide policies	
v.2.0	Gareth Kitchen	Updates to reflect 2020 process updates.	17/12/2019

Contents

1. Introduction

This policy sets out the requirements applicable to the processing of personal data in the Tes group of companies. It has been written with consideration all currently applicable privacy law including the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communication Regulations 2003.

When we process personal data we must always consider how we will be **transparent** with individuals whose personal data we process and **accountable** for the processing which we will carry out on that personal data.

The policy is applicable to all personal data processed within the Group.

The latest version of this policy is available at all times on the company Intranet site.

2. General Guidance

- Whenever using personal data, it should be treated with the utmost confidentiality at all times.
- Continually understand what personal data you process and the reasons for processing it. If we are collecting data we do not use, this should be escalated to the Information Governance Team.
- Before you start collecting new personal data, or start using personal data for a different reason than it was collected for, understand the privacy implications of this by carrying out a formal assessment.
- If you receive a request from an individual asking to enforce one of their Data Subject Rights, contact the Information Governance Team Immediately.
- If you think you may have discovered a personal data breach or have any concerns regarding the use of personal data in the organisation, report these immediately to the Information Governance Team.
- If you are unsure about what you should be doing with personal data, ask for guidance!

3. Key Definitions

To understand the requirements of this policy, it is important that all individuals understand the following key terminology.

1. **Personal data**
   a. Any information which relates to an identifiable individual. Including their basic identifiers and contact details, identification numbers or references, information about their location, behaviour or physiology and all online identifiers.
2. **Data Subject (individual)**
   a. The person about whom personal data relates to. Within this document they will be referred to as the **'individual'**
3. **Processing**
   a. Any operation or set of operations that is performed on personal data. This includes collection, storage, and organisation, use disclosure and alteration, restriction, erasure and destruction.
4. **Controller**
   a. This is the term used to define the organisation which, either alone or in conjunction with another, decides how personal data will be used.
5. **Processor**
   a. This is the term used to define an organisation who processes personal data on behalf of a controller.
6. **Special Category Personal Data**
   a. Where personal data is of a sensitive nature, controllers and processors must hold it in the highest for protection. The special categories or personal data include data relating to an individual's;
      i. Ethnicity, race, religious or philosophical beliefs,
      ii. Political opinions or trade union membership,
      iii. Genetic data and biometric data which will be used for identification purposes,
      iv. Mental or physical health,
      v. Sex life or sexual orientation,
      vi. Criminal convictions or offences.

7. Data Protection Officer (DPO)

a. This is the individual who is responsible for providing data protection information and advice as well as monitoring compliance will all relevant privacy law. Within this document they will be called the **DPO**.

4. Data Protection Principles

Since the earliest Data Protection Law, key principles have defined and directed how personal data should be processed. Under the GDPR we have 6 core principles underpinned by the principle of **accountability**.

Accountability.

The principle of accountability should be seen as underpinning everything which we do with personal data. This means that we should be able to consistently demonstrate how we process all personal data in compliance with the 6 Data Protection Principles.
The 6 Data Protection Principles are;

1. Lawfulness, fairness and transparency

a. Personal data must be processed in a lawful, fairly and in a transparent manner in relation to the individual.

2. Purpose limitation

a. Personal data musty be collected for specific, explicit and legitimate purposes. We should not process personal data in a manner that is incompatible with those original purposes.

3. Data minimisation

a. When collecting personal data it must be adequate, relevant and limited to what is necessary in relation to the purpose it is being collected for.

4. Accuracy

a. We must take reasonable steps to ensure the personal data we process is as accurate up to date as possible. If personal data is incorrect or inaccurate it should be corrected, completed or erased.

5. Storage limitation

a. Personal data should only be kept for as long as is necessary for the purpose it is being processed for.

6. Integrity and confidentiality

a. Personal data should be processed in a way that ensures appropriate security against unauthorised processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5. Lawful Basis for processing

Whenever we process personal data, we must do so in a lawful manner. Each processing activity we undertake must have a lawful basis for processing. There are six lawful basis' for processing, each basis is equal and should be assigned on a processing by processing basis. The six lawful basis for processing are as follows;

1. The individual has given their **consent** to one or more processing activities,
2. The processing of personal data is required for the performance of or entrance into a **contract** with the individual,
3. The controller must process the individual's personal data to comply with a **legal obligation**,
4. Processing is necessary for the purposes of the controller or a third parties **Legitimate Interest** where those interests are not incompatible with the rights and freedoms of the individual,
5. Processing is necessary in order to protect the **vital interests** essential in the protection of the individual or another individual's life,
6. Processing is necessary for performing a task in the **public interest** or in the exercise of an official appointment.

At ABC Teachers, Smart Teachers and Vision for Education, the majority of our processing is on the basis of the second lawful basis, performance of or entrance into a contract with a data subject.

ABC Teachers, Smart Teachers and Vision for Education will only send direct-email-marketing messages to individuals on the basis of consent. There are no instances where ABC Teachers, Smart Teachers and Vision for Education will use our legitimate interests, also known as a soft opt-in, to undertake direct-email-marketing messages to individuals . All consents are mastered and amendable via the preference centre on Tes.com.

ABC Teachers, Smart Teachers and Vision for Education record the lawful basis for processing alongside each activity in our Record of Processing Activities (RoPA) documented on spreadsheets stored in Google Drive. Where special category personal data is processed, the organisation must have a further basis to process this personal data.
To understand what to do when you are processing special category personal data, please see **Section 13** of this policy.

6. Rights of the Data Subject

Controllers and processors are expected to support and provide mechanisms for individuals to uphold their Data Subject Rights. Individuals have 8 core data subject rights, but they are not all absolute rights. The applicability of individuals' data subject rights depends on factors such as the Lawful Basis for processing and the Data Protection Principles.

Individuals have the following data subjects' rights;

- To be **informed** about how their personal data is used,
- **Access** to their personal data,
- **Rectification** or completion of their personal data
- **Erasure** of their personal data.
- **Restrict** how their personal data is processed.
- **Port** their personal data to another controller.
- **Object** to the use of their personal data.
- Rights relating to use of **automated decision** making, including profiling, using their personal data.

When a data subject makes a request exercising one or more of their rights we must respond to that request within one month. In exceptional circumstances this can be extended.

At ABC Teachers, Smart Teachers and Vision for Education, each company dealing with Data Subject Request will follow their own process led by their Data Champions. Where individuals have questions about their process, the Data Champions should be the first point of contact.

Each team will maintain accountability for the requests they are processing by recording them in access controlled spreadsheets. These records should be made available to the Technology Governance Team where requested.

Receiving a request from an individual

Any individual can make a request asking ABC Teachers, Smart Teachers and Vision for Education to uphold one of their Data Subject Rights defined above.

Unlike previous laws, these requests do not need to be in writing so staff need to be aware that a request could be received in person, online, by email, on the phone, via social media or in writing. If you are unsure whether an individual is making a request in line with their Data Subject Rights you should contact your Data Champion immediately.

Each team handling requests will maintain and disseminate through their team a process for handling requests received from individuals. These processes should be made available to the Technology Governance Team where requested.

Not all rights are absolute so when complex requests are received the Data Champion actioning the request should alert the Information Governance Team immediately. This should be done via email to the dpo@tes.com email address.

7. Data Controller or Data Processor?

The organisation has different obligations where we act as a controller compared to when we act as a processor. We are always obliged to understand what personal data we process regardless of whether we decide how that data is processed or whether another organisation makes that decision.

When a new third party is contracted, or we are contracted to a third party, we must maintain a record of this relationship along with information about the processing activities which we will undertake in the course of that relationship. This is called a Record of Processing Activities (RoPA). More information about this can be found in section 8 of this policy.

Prior to the on boarding of any new third party that will process personal data, the Technology Governance

Team, Legal Team and where relevant, the PMO, should be made aware.

Any new third parties that are on boarded will have their Data Processing Agreements, or equivalent, reviewed by Legal who will liaise with the Information Governance Team. These agreements will be stored alongside their main terms and other associated documentation in the OneTrust Vendor Risk Management Module. Access to these documents will be on a strict, need to know basis.

Unless you have been cleared to do so, no employee should sign a Data Processing Agreement or similar without agreement from the Technology Governance or Legal Teams.

8. Records of Processing Activities

All organisations processing personal data on a permanent basis are legally required to maintain a Record of Processing Activities (RoPA). This is a living document which should change and evolve as we add, amend or cease processing activities. The ICO requires that this record is granular and extensive which means every operational unit must be involved in its creation and maintenance.

All departments are required to understand the processing activities they undertake and inform the Information Governance Team of any changes via their Data Champion.

The organisation's RoPA is stored on spreadsheets stored in Google Drive and this is maintained by the Technology Governance Team. Each Data Champion is responsible for the upkeep and accuracy of their RoPA's and will be asked to confirm they have done this on a quarterly basis. Where necessary, assistance with this activity will be provided by the Technology Governance Team.

9. Data Protection by design and by default

Data Protection by design and by default is underpinned by an understanding of the risk apparent to individuals by processing their personal data. Before a new processing activity is undertaken, the organisation should understand how the data protection principles, security and data subject rights will be upheld. By understanding how this will be actioned, the organisation will design new processing activities with sufficient safeguards, protection and security implemented as standard.

This approach can be achieved in many ways, from designing systems with the highest levels of security as standard, getting assurances from third parties regarding their compliance, and risk assessing new technologies prior to their use.

A vital tool in implementing data protection by design and by default is a risk assessment called a Data Protection Impact Assessment, or DPIA.

ABC Teachers, Smart Teachers and Vision for Education process DPIA's using spreadsheets stored in Google Drive. Data Champions should recognise and raise a request with the Information Governance Team when they need to undertake a DPIA. Where required, the Information Governance team will advise and guide on DPIA's but these assessments must be led by Data Champions.

When to complete a Data Protection Impact Assessment (DPIA)

Although not required for every processing activity, when a type of processing is likely to result in a high risk to the rights and freedoms of individuals, a DPIA shall be carried out before processing begins.

A DPIA is deemed to be required where a new processing activity will include at least two of the following 12 actions;

1. Systematic and extensive profiling or automated decision-making to make significant decisions about people.
2. Process will include special category data or criminal offence data on a large scale.
3. Systematic monitoring of a publicly accessible place on a large scale.
4. The use new technologies or applications.
5. The use of profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
6. The carrying out of profiling on a large scale.
7. The processing of biometric or genetic data.
8. The combination, comparison or matching of data from multiple sources.
9. Processing of personal data without providing a privacy notice directly to the individual.
10. Processing of personal data in a way which will involve tracking individuals' online or offline location or behaviours.

11. The processing of children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
12. The processing of personal data which could result in a risk of physical harm in the event of a security breach.

Should a processing activity fulfil two of the above actions, the Information Governance Team should be alerted so that a DPIA can be activated. This should be done via email to the dpo@tes.com email address. This will alert the Data Champion who will be charged with completing it.

10. Security of Processing

The level of security required shall be applied, and maintained, based on the level of risk posed by the processing activity.

The minimum standard of security shall be the level set out in the information security policies.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

As any approved codes of conduct, or certifications are developed and approved by national or continental supervisory authorities, the application of these mechanisms shall be assessed and where relevant approved by the DPO.

11. Processing special categories of personal data

The processing of personal data which reveals an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, or data relating to criminal offences or convictions is prohibited unless an exemption applies. The Data Protection Act 2018 provides specific details regarding the exemptions and where they apply.

Should your department be processing, or planning on processing special category personal data, the Information Governance Team should be alerted. This should be done via email to the dpo@tes.com email address.

12. Sending electronic marketing messages to individuals

When we send electronic communications advertising our services direct to individuals, there are differing rules when we do so for corporate subscribers and for individual subscribers.

An electronic communication is any information sent between us and a subscriber over a phone line or internet connection. This includes phone calls, text messages, video messages, emails and internet messaging.

The differing rules in place for subscribers differ further depending on the method of communication. This means that when we email an individual subscriber, we have different obligations compared to when calling a corporate subscriber.

Generally, the rules on marketing to companies are not as strict as when we communicate with individuals. In all cases we will require an individual's consent to market to them.

Prior to sending any direct marketing email, the Marketing Team should be contacted for their advice and guidance to ensure the proposed activity aligns with their processes. Where emails will be sent, they may only be sent where an individual's consent is recorded and valid on the tes.com preference centre.

Where you or your team is sending new marketing communications, the Information Governance Team should be made aware. This should be done via email to the dpo@tes.com email address.

13. Restricted transfers of personal data outside of the EEA

A transfer of personal data to a country outside of the EEA (European Economic Area) can only take place under limited circumstances. A transfer of personal data outside of the EEA is deemed a restricted transfer where;

1. Personal data is sent, or made accessible, to a recipient to whom the GDPR does not apply; and
2. The recipient is a separate organisation or individual. The recipient cannot be an employee of the company but can be a company within the same group.

A transfer is not the same as transit, where personal data is just electronically routed via a none-EEA country

and the personal data is from one EEA country to another, no transfer is deemed to have taken place.

In any event that a processing activity may include the transfer of personal data outside of the EEA, the Information Governance Team should be alerted. This should be done via email to the dpo@tes.com email address.

14. Breach notification

A personal data breach is an event where there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration disclosure or access to personal data.

If you think you have discovered a personal data breach, you should raise this immediately with your Data Champion.

Unless a Tes employee or contractor has been cleared to contact the ICO, all Personal Data Breaches should be reported internally only.

15. Incidents

If, during the performance of your job, you are made aware of a breach of this policy please report the incident via email to the dpo@tes.com email address.

16. Contacting your Information Governance Team

Should you have a specific question for the Information Governance Team or a Data Champion at a Tes Group company, please address it to the following email address.

Tes Global	dpo@tes.com
Vision for Education	dpo@visionforeducation.co.uk
SMART	dpo@smartteachers.co.uk
ABC	dpo@abc-teachers.co.uk
Tes Institute	dpoinstitute@tesglobal.com
THE	dpothe@timeshighereducation.com

---------- End of Document ----------