**GDPR – General Data Protection Regulation May 2018**

Full details of the 12 Steps recommended by the Information Commissioners Office to be evaluated to ensure compliance with GDPR are found on ico.org.uk and are as follows.

Where the step has an implication for the TF this is detailed, else Not Applicable (N/A) is indicated.

Full details, definitions and reasoning are given in the Appendix

1 – Awareness .

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

2 – Information that we hold.

* Single Central Register – a legally required document detailing personal, safeguarding and training qualifications & status for all tutors employed by the Tutorial Foundation Day School.
* Admissions Register – a legally required document that details personal data pertaining to students, family/carer contacts and their enrolment status.

These elements of data are maintained and managed electronically by the administrative office of the Tutorial Foundation Day School and are overseen by the school’s Senior Leadership Team and Safeguarding Advisory Board. The files are accessible through secure logins.

* Safeguarding Information pertaining to Children of concern or Children at risk; medication details and SEND information.

This information is kept in secure files in a locked cabinet and is accessible only by the Senior Leadership Team (all Designated Safeguarding Leads), by the Welfare Officer and Administration Officer.

* Payroll information necessary to pay salaries to tutors and associated pension, and tax.
* Customer information necessary to invoice for products & services, and to receive payments.
* Supplier information necessary to place orders and make payments for goods & services received.

This information is all held securely in a financial accounting package that is held on the Tutorial Foundation server. Access is strictly limited by secure logins.

3 – Communicating Privacy Information - Privacy Statement.

The Tutorial Foundation collects and stores personal data to meet regulatory requirements to safeguard the wellbeing of its’ students and staff. Any such data is used internally and is accessible only via restricted access sign-on and is not shared externally except as required to meet regulatory requirements.

4 – Individual’s rights, (to be informed; access; rectification & deletion)

Data is stored in easily accessible files, any decision regarding deletion of data would be ratified by the Safeguarding Advisory Board. Deletion is subject to regulatory requirements at the time of the deletion request.

5 – Subject Access request .. N/A

6 – Lawful basis for processing persona data ..

All data held, is held for statutory/regulatory purposes and the school cannot operate without this information. The TF does not “process” data. Requests for deletion of data will have to comply with the prevailing legislation at the time.

7 - Consent

Consent for photographs/video to be taken MUST be Opt-in consent and not Opt-out, relevant for staff & students & is in line with our policies.

Consent to process data (we do not) .. N/A

8 – Children (age verification for online services) .. N/A

9 – Data breaches, (risk to rights & freedoms) .. N/A

10 – Data Protection by design, and Data Protection Impact Analysis

(DPIA) (where data is processed) .. N/A

11 – Data Protection Officers .. N/A

12 – International (operation across borders) .. N/A

Policy Sign off and review

|  |  |  |
| --- | --- | --- |
|  | By whom | Date |
| Policy signed off by | Tim Low | 28.02.2018 |
| Reviewed by | Tim Low/Marion Veal | 9.10.2019 |
| Next Review By | Safeguarding Advisory Board | 31.10.2020 |

**Appendix – Definitions, explanation and reasoning**

1. Awareness

What information does the GDPR apply to?

* **Personal data**

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

* **Sensitive personal data**

The GDPR refers to sensitive personal data as “special categories of personal data” (see Article 9). Examples of special categories are as below,……

This is because special category data is more sensitive, and so needs more protection. For example, information about an individual’s:

* race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.

The Tutorial Foundation does NOT retain any such “sensitive” data.

## Who does the GDPR apply to?

* The GDPR applies to ‘controllers’ **and** ‘processors’.
* A controller determines the purposes and means of processing personal data.
* A processor is responsible for processing personal data on behalf of a controller.

The TF data is subject to oversight by the Safeguarding Advisory Board And administered by the administration office.

1. Information that the Tutorial Foundation holds

* Single Central Register – a legally required document detailing personal, safeguarding and training qualifications & status for all tutors employed by the Tutorial Foundation Day School. The SCR records of tutors who leave employment are archived and may be deleted.
* Admissions Register – a legally required document that details personal data pertaining to students, family/carer contacts and their enrolment status. The data may be archived but may not be deleted.

These elements of data are maintained and managed electronically by the administrative office of the Tutorial Foundation Day School and are overseen by the school’s Senior Leadership Team and Safeguarding Advisory Board. The files are accessible through secure logins.

* Safeguarding Information pertaining to Children of concern or Children at risk. SEND information. (Note: if we did have any students who are eligible for free school meals or pupil premium this data would have to be treated in the same restricted access manner.)

This information is kept in secure files in a locked cabinet and is accessible only by the Senior Leadership Team (all Designated Safeguarding Leads), by the Welfare Officer and Administration Officer.

* Payroll - personal and banking details of all employees required to process salary and HMRC submissions

These elements of data are maintained and managed electronically by the administrative & payroll office of the Tutorial Foundation. The files are accessible through secure logins.

1. Communicating Privacy Information

GDPR requires that organisations Collect and use personal information fairly and transparently

The first principle of data protection is that personal data must be processed fairly and lawfully. The DPA says that in order for the processing to be fair, the data controller (the organisation in control of processing the data) has to make certain information available to the data subjects (the individuals whom the data relates to), so far as practicable:

* who the data controller is;
* the purpose or purposes for which the information will be processed; and
* any further information which is necessary in the specific circumstances to enable the processing to be fair.

Being transparent by providing a privacy notice is an important part of fair processing.

Therefore the main elements of fairness include:

* using information in a way that people would reasonably expect
* thinking about the impact of your processing. Will it have unjustified adverse effects on them? and;
* being transparent and ensuring that people know how their information will be used.

To cover all these elements you will need to consider the following issues when planning a privacy notice:

* What information is being collected?
* Who is collecting it?
* How is it collected?
* Why is it being collected?
* How will it be used?
* Who will it be shared with?
* What will be the effect of this on the individuals concerned?
* Is the intended use likely to cause individuals to object or complain?

The Tutorial Foundation collects and stores personal data to meet regulatory requirements to safeguard the wellbeing of its’ students and staff. Any such data is used internally and is accessible only via restricted access sign-on and is not shared externally except as required to meet regulatory requirements.

1. Individuals Rights

Procedures are required to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

The GDPR includes the following rights for individuals:

•the right: to be informed; of access; to rectification; to erasure; to restrict processing; to data portability; to object; and not to be subject to automated decision-making

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements.

Regarding how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

The right to data portability is new. It only applies:

* to personal data an individual has provided to a controller;
* where the processing is based on the individual’s consent or for the performance of a contract; and
* when processing is carried out by automated means.

Data is stored in easily accessible files, any decision regarding deletion of data would be ratified by the Safeguarding Advisory Board. Deletion is subject to regulatory requirements at the time of the deletion request.

The right to data portability is is not applicable for any data held by the Tutorial Foundation.

1. Subject Access requests

This area is NOT APPLICABLE to the Tutorial Foundation for two reasons: we do not receive any access requests; data held is minimum required and would be easy to share if requested.

1. Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals’ rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

All data held, is held for statutory/regulatory purposes and the school cannot operate without this information. The TF does not “process” data. Requests for deletion of data will have to comply with the prevailing legislation at the time.

1. Consent
2. Consent for photographs/video to be taken MUST be Opt-in consent and not Opt-out, .. for staff & students & is in line with our policies

b. The Tutorial Foundation does not “process” or share personal data and as such does not need to obtain “consent”.

If you are offering online services to children and want to rely on consent for your processing, you need to adopt age-verification measures and seek parental consent for children under 16 (or the age specified in UK law).

c. The TF does not offer online services directly to children. We are aware that we can only seek consent if we have age-verification and parental-consent measures in place.

1. Children

If your organisation offers online services (‘information society services’) to children and relies on consent to collect information about them, then you may need a parent or guardian’s consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16

The Tutorial Foundation does not online services to children and therefore this is NOT APPLICABLE to the TF.

1. Data Breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

The nature of the data held by the TF does not impact upon any possible risk to rights and freedoms of individuals (as defined), this means that this issue is NOT APPLICABLE to the TF..

NB… beware IT Hardware “end of life procedures”, .. data held on hard drives etc. must be wiped before disposal.

1. Data Protection by Design and Data Protection Impact Assessments

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

* where a new technology is being deployed;
* where a profiling operation is likely to significantly affect individuals; or
* where there is processing on a large scale of the special categories of data.

The nature of the data held, and that of processing by the TF means that this issue is NOT APPLICABLE to the TF

1. Data Protection Officers

You should consider whether you are required to formally designate a Data Protection Officer (DPO). You must designate a DPO if you are:

* a public authority (except for courts acting in their judicial capacity);
* an organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
* an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions.

The nature of the organisation the Tutorial Foundation means that this issue is NOT APPLICABLE to the TF

1. International

The Tutorial Foundation does NOT operates in more than one EU member state, the TF does NOT carry out cross-border processing – the TF does NOT have establishments in more than one EU member state and the TF does Not carrt out processing which substantially affects individuals in other EU states.

The nature of the organisation the Tutorial Foundation means that this issue is NOT APPLICABLE to the TF