THE TUTORS' ASSOCIATION

TABLE OF CONTENTS

1. GDPR Action Plan

1. Accountability, raise awareness and create alignment

Both Private Tutors and Tutoring Agencies must ensure that anyone who touches data are aware of the law, impacts and potential risks.

Accountability is one of the data protection principles - it makes you responsible for complying with the GDPR and says that you must be able to demonstrate your compliance. You need to put in place appropriate technical and organisational measures to meet the requirements of accountability.

There are a number of measures that you can, and in some cases must, take including:

- adopting and implementing data protection policies;
- taking a 'data protection by design and default' approach (see below, Privacy and Security Policy)
- putting written contracts in place with organisations that process personal data on your behalf;
- maintaining documentation of your processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- adhering to relevant codes of conduct and signing up to certification schemes.

Accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place.
Being accountable can help you to build trust with individuals and may help you mitigate enforcement action.

2. Data audit

Understand and document what data you hold, where it came from, how it was collected and with whom and how it is shared. Identify all sources of data and all types of data relationships (e.g., third-party tools and tags on sites).
Questions to be asked may include:

- **Who** are our data subjects? Who has access to sensitive data?
- **Where** do we keep their personal data? Where do we transfer personal data to?
- **Why** is personal data under our control (for what legitimate purpose)? Why do we share it with third parties? Do third parties share it with other entities? If so, who, how many and to what purpose?
- **When** are we keeping personal data until? When do we share personal data with others?
- **What** mechanisms do we have in place to safeguard personal data?
- **How** is data being processed? How long should it be kept?

3. Legal basis for processing

Identify and define the legal basis for you or your organisation to collect data and make it clear in your Privacy Notice

4. Notices and Policies

Do a full review of the current privacy policies (different to privacy notices) and privacy notices you have in place and ensure that these will align with requirements under GDPR. If you don't have any of these in place, consider implementing them. (See points 'Privacy and Security Policy' and 'Privacy Notice' on this document)

At a minimum, touch on the following points:

- the identity of the controller (who process the data) and of the data protection officer (if applicable)
- conservation period (how long data will be kept, other than for legal or financial bases)
- how are data subject's rights being observed
- recipients and transfers of data (such as Dropbox, Google docs, Mailchipm, etc)
- state the right to withdraw consent at any time
- explain your legitimate interest or of a third party (if relevant) in the collection of the data

5. Managing consent

A data subject never relinquishes their rights, so managing their consent becomes extremely important. You will need to ensure that consent is sought, obtained and recorded according to new guidelines, and that you are able to respond to inquiries regarding consent. At a minimum, you will need to:

- request and obtain the data subject's affirmative and detailed consent for you to hold their data
- discontinue processing activities if the data subject denies consent
- provide a mechanism for data subjects to withdraw consent
- obtain affirmative consent from a child's (under age of 13) parent or guardian
- Obtain affirmative consent from the data subject the they are happy for you to contact them (in accordance with The Privacy and Electronic Communications Regulations (PECR))

2.Identifying The Legal Basis

There are six legal bases for processing data under GDPR, an organisation only needs one of these to be identified as their legal basis for processing data.
Before you hold or process data on a Data Subject, you must make sure that you have a lawful basis for doing so.

These are the different lawful bases:
Consent
Contract
Legal Obligation
Vital Interests
Public Task
Legitimate Interests

The 'legitimate interests' lawful basis is probably the one upon which most organisations currently rely. The term 'legitimate interests' means that an organisation is free to hold or process data in a way that the individual could reasonably expect, and which apply to the relationship between the controller and the subject.

For example, if a new person enquires about your services, a course or event you are promoting, they could reasonably expect you to use the information they have provided in order to send them further details about the course. This is the 'common sense' approach to data processing.

However, there are some provisions. The first is that organisations may only process the data in a way that the individual might reasonably expect.

The second proviso is that legitimate interest only applies when there is a minimal risk of any impact on the individual's privacy. So, if you don't have appropriate security measures around your email address book or indeed any emailing lists or where and how they are stored, you could find ourselves in breach.

The legal basis should be clearly delimited in a Privacy and Security Policy as well as on the Privacy Notice.

3.Data Subject Rights

Right to Access
Anyone who has their data stored by us can request to see a copy of this data. This is called a Data Subject Access Request. This would include everything that is stored about that person.

If the subject makes the request electronically, the information must also be supplied electronically. It must be clear as to whom the person should contact to ask for this information. The information must also be supplied within 30 days of receiving the request.

A Data Subject Access Request does not mean only sharing some information with the Data Subject. It means letting them see everything you hold on them. This is to encourage organisations to really think before they write something down.

Right to Rectification
It should be clear whom data subjects should contact if any data is wrong; this should be made clear in your Privacy Notice.

It is important that when someone has informed you of incorrect information, that it is updated within one month. If it is particularly complex then we will be allowed up to two months, however this is an exception.

If the data has been shared with anyone else then these parties need to be informed, e.g. if we have shared Gift Aid information with HMRC.

Right to Erasure
The 'Right to Erasure', or the 'Right to be Forgotten' means that a data subject can request for all of their information to be erased from your systems.

This person may have previously given their consent for data to be held, but has subsequently withdrawn it and is requesting that their data be erased. This would mean that searching for that person would generate no results or data.

There are exceptions to this if information is required for archive or historical purposes such as:

- Needing to hold financial records (as per HMRC's instructions, is up to 6 years)
- There is another Data Subject whose data will be affected by the deletion
- The data may be necessary for Child Protection purposes
- You may have another lawful basis for processing the data

If this data has been shared by you with any other parties then they also need to be informed that the data needs to be erased. You will also need to make any consequences of erasure clear to the individual, e.g. that you will not be able to schedule them on for lessons if you cannot hold the necessary data.

Should a case arise, the request must be actioned within a reasonable time. There will also be your own terms for data retention to consider. For example, you may have backups of your data and it is not possible to go through each backup and remove all references to a data subject who has requested a right to be forgotten. However you should make it clear in your Privacy Notice how long information would be stored

Right to Restrict Processing
The Right to Restrict Processing is not the same as the Right to Object or the Right to Erasure. It does not mean that you have to delete the data, only that you are not allowed to do anything other than store it. Individuals will only exercise their right to restrict processing under specific circumstances. These include:

- Someone has told you that their data is incorrect. Right to restrict processing requires that you do not process this data until it has been corrected.
- Someone has exercised their right to object, but you need time to find out whether you need to continue processing that information for a reason which overrides that individual's request.

If further processing is against the law, but the individual has requested that you restrict processing instead of deleting the data.

You no longer need the data but the individual wants you to hold onto it as they may need it for legal reasons.

If you share the data with any third parties, you must also inform them of the processing restrictions. You must also inform them and the individual when and if the restriction is lifted.

Right to Object
An individual can object at any time to you using their personal information for:

- Direct Marketing. If an individual objects to you using their data to contact them for this purpose then you must cease immediately. There are no exemptions.
- Scientific, historical, research or statistical purposes. You can have an exemption from this if you have a legitimate need to keep processing it, e.g. reports to HMRC.

You must offer a way for individuals to object online. This could be as simple as providing a dedicated email address for data subjects to use for all data requests.

Right to Data Portability
The Right to Data Portability means that an individual can ask for their data to be transferred from one IT system to another, in a safe, secure way which ensures confidentiality.

You must ensure that the data is transferable for an individual in a secure manner.

4.Children Under 13 And Vulnerable Adults

The GDPR requires that parents or guardians must give permission for organisations to offer an online service in order to hold or process the personal data of those under the age of 16.

However, there is a provision within the GDPR for member states like the UK to lower this age if they see fit. In the UK, the 'age of consent' for allowing the storage of their own data is 13.

When the child reaches 13 they themselves need to give their own permission, as well as allowing you to keep holding the older data.

Although their parents or guardians may give permission on the child's behalf, you should still try to ensure that you are taking special care with children's data. You should also make some reasonable effort to ascertain that adult giving proxy permission actually does have legal parental responsibility. This will likely not be the case for grandparents, older siblings, or step-parents, unless a court order has been made.

Keep in mind that consent is only one of the six possible lawful bases, and may not always be the most appropriate when dealing with a child. Unless you can be absolutely sure that the child fully understands, you should seek consent from an adult with parental responsibility.

*Parental consent is not required if the child is accessing counselling or preventative services.

Vulnerable Adults
Your Privacy Notice and any other documentation should be written in clear, plain language to make it easy for everyone, including children and adults with learning disabilities, to understand and give their consent. However, you many need to cater to people who, through more severe disability or illness, are not able to do so.

Most vulnerable adults or their companions will have approached you for a services, and you will be holding their data to make this possible. This would come under the lawful basis of Legitimate Interests for processing. For example, you could not tutor them in their home without keeping a record of their address.

If the person's carer, Power of Attorney or next of kin has already given their permission for you to store the vulnerable adult's data, and the way in which you are going to use said data has not changed, you do not need to seek fresh consent. However, if you do not have a record of prior consent or you use of the data has changed; you will need to approach them to ask for permission just as you would with anyone else should Consent be the lawful basis. You should make a clear note that consent was granted by proxy, who recorded it, and when. This consent should be revisited if the vulnerable adult's situation changes.

5.Should You Appoint A Data Protection Officer?

The GDPR introduces a duty for you to appoint a data protection officer (DPO) if you are a public authority, or if you carry out certain types of processing activities.

DPOs assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

6.Privacy And Security Policy

A Privacy and Security Policy is different to a Privacy Notice.

This is for internal use of those working with you and within your organisation documenting who has access, where the data is kept, how long it is kept for, and in what format as well as the purposes and methods of collecting and using the data and make it clear to all employees that failing to comply with it, may put you at risk of a breach. This should be added to the employee's handbook, given to any new employee, etc.

It is your responsibility to treat the data of others as you would wish our own to be treated. You may not only store information electronically, it is important that it is stored securely. Taking precautions such as password protecting data before it is transferred to an external device is important. A full database of customers may fill up a very small part of a USB stick, yet without common sense practices it can easily be left on the stick indefinitely, or copied onto a shared computer. You must ensure that if any person has an electronic copy of people's data, they have to make sure it is securely deleted from any computers or media when it is no longer used.

Data held locally on USB, CD, or memory cards must be handled carefully. You must give clear and precise information about how to responsibly, securely and in accordance with your guidelines, to all of those handling data carefully.

You may often print out information to take to a meeting but if this contains personal data then make sure that it is securely stored or, ideally, destroyed.

If you store data on cloud based such as Google Drive or DropBox then it should be clear as to who has access to this information.

7.BYOD (Bring Your Own Device)

BYOD raises a number of data protection concerns due to the fact that the device is owned by the user rather than the data controller (You). It is crucial that you ensure that all processing of personal data which is done under your name remains in compliance with the DPA.

It is important to remember that you must remain in control of the personal data for which you are responsible, regardless of the ownership of the device used to carry out the processing.

What are the risks?
The underlying feature of BYOD is that the user owns, maintains and supports the device. This means that you will have significantly less control over the device than it would have over a corporately owned and provided device.

You will need to assess: what type of data is held; where data may be stored; how it is transferred; potential for data leakage; blurring of personal and business use; the device's security capacities; what to do if the person who owns the device leaves their employment; and how to deal with the loss, theft, failure and support of a device.

The Data Protection Act 1998 (DPA) requires that the data controller (You) must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The starting point should be to audit the types of personal data you are processing and the devices, including their ownership, which will be used to hold it. An important question to consider is which personal data can be processed on a personal device (that is one owned by an employee) and which must be held in a more restrictive environment. You must also consider whether employees' use of their own devices will mean that the employer ends up processing non-corporate information about the owner of the device and possibly others who use it, for example family members. Consider whether the controls you have in place are appropriate for any sensitive personal data being processed.

It is important that users connecting their own devices to your IT systems (if any in place) clearly understand their responsibilities.

You should Implement and maintain an Acceptable Use Policy to provide guidance and accountability of behaviour; consider the need for a Social Media Policy if BYOD leads to an increased use of social media; be clear about which types of personal data may be processed on personal devices and which may not.

Where personal data is stored on a device it will be important to consider the safe and secure deletion of the data throughout the lifecycle of the device, and particularly if the device is to be sold or transferred to a third-party.

We would recommend to anyone who uses their own devices to process data to:

- use a strong password to secure their devices
- use encryption to store data on the device securely
- ensure that access to the device is locked or data automatically deleted if an incorrect password is input too many times
- ensure that the device automatically locks if inactive for a period of time
- make sure users know exactly which data might be automatically or remotely deleted and under which circumstances; and

- maintain a clear separation between the personal data processed on behalf of your organisation and that processed for the device owner's own purposes, for example, by using different apps for business and personal use.

8.Privacy Notice

A Privacy Notice should be written in clear, plain language. It must be readily available, free of charge, and easy to understand. It should be available on your website or accessible on request.

The Privacy notice must include the identity and your contact details well as the person or persons responsible for overseeing Data Protection within your organisation.

It must outline all your plans for an individual's data. This means setting out exactly what data you collect exactly what will be done with it and how and where it will be stored.

You must list any third parties who will have access to the data, e.g. HMRC or Data Processors (software used to manage customer data), Google Drive or Dropbox; newsletter editors such as Mailchimp; payroll processors, auditors, etc.

The policy should clearly state their right to withdraw consent at any time, and their right to lodge a complaint with the ICO.

You must also provide a clear mechanism for subjects to execute their rights such who do they need to contact in their data needs amending, or deleted, etc.

9.Data Breach Plan

A data breach occurs whenever the security of personal data is compromised. This could be as simple as sending an email to the wrong person, leaving a folder containing paper financial record on the bus, or wiping a computer drive which contained important records. It does not matter if the breach occurs by accident or as a result of deliberate actions. You should have a clear breach plan so that in case a breach occurs, data subjects are aware of what you intend to do.

Some breaches result possibly in paying a notification fee to the regulatory authority: in the UK's case, the ICO. The ICO is also who you need to inform if you were to experience a significant data breach. This must be done so within 72 hours, and you must keep a record of the breach as well.

You do not necessarily need to let the individuals know, however, you must do so if there is a high risk of an adverse effect against their rights and freedoms.

10.The Privacy And Electronic Communications Regulations (PECR) And What Counts As Consent?

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the GDPR. They give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- marketing calls, emails, texts and faxes
- cookies (and similar technologies)
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings

Some of the rules only apply to organisations that provide a public electronic communications network or service. But even if you are not a network or service provider, PECR will apply to you if you:

- market by phone, email, text or fax;
- use cookies or a similar technology on your website; or
- compile a telephone directory (or a similar public directory)

What counts as consent?
You will often need a person's consent before you can send them a marketing message. If you do need consent, then – to be valid – consent must be knowingly and freely given, clear and specific. It must cover both your particular organisation and the type of communication you want to use (eg call, automated call, fax, email, text). It must involve some form of very clear positive action – for example, ticking a box, clicking an icon, or sending an email – and the person must fully understand that they are giving you consent. You cannot show consent if you only provide information about marketing as part of a privacy policy that is hard to find, difficult to understand, or rarely read.
The clearest way to obtain consent is to ask the customer to tick an opt-in box confirming they are happy to receive your marketing calls, faxes, texts or emails.

You should keep clear records of what a person has consented to, and when and how you got this consent, so that you can demonstrate compliance in the event of a complaint.

You should be very careful when relying on consent obtained indirectly (consent originally given to a third party). You must make checks to ensure that the consent is valid and specifically identifies you. Generic consent covering any third party is not enough.

Remember that the customer is entitled to withdraw their consent at any time. You must make it easy for people to withdraw consent, and tell them how.

For further information, see ICO's guidance on direct marketing and guidance on consent.