



Home-School Tutoring UK Data Protection Overview for Tutors (Key Principles)

Introduction

Since 2018 – and possibly before – you’ve probably heard a lot about the General Data Protection Regulation (GDPR). It’s a law from the EU that sets out how organisations can use people’s personal data. Everyone needs to understand and follow the policies and procedures for handling personal data and lead by example in how they handle the data in their care.

While Brexit means that EU law doesn’t generally apply in the UK from 1 January 2021, the GDPR has been passed into UK law as the UK GDPR. This is nearly identical to the EU’s version of the law and will make little difference to most schools or education providers unless they use processors that are based or store data outside the UK or have students or staff who spend some part of the year living in the EU.

Supervisory authorities

Under the UK GDPR, the only supervisory authority (data protection regulator) is the ICO (Information Commissioner’s office), which provides a lot of guidance on data protection. HomeSchool Tutoring UK and all the regional Home-School Tutoring offices are registered with the ICO.

Let’s have a look at the ICO website for clear information about what constitutes personal data:
<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/>

One of the most helpful aspects of the GDPR is the clarity with which it identifies what personal data is. It includes, of course, the obvious identity markers such as: name, address, photo, phone number, signature, email address, job role, age, ethnic identification.

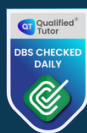
Now let’s look at what is meant by identifiability on the ICO website:

“What is identifiability?”

If you can distinguish an individual from other individuals, then that person is ‘identified’ or is ‘identifiable’. Often an individual’s name together with some other information will be sufficient to identify them.

A name is perhaps the most common means of identifying someone. However, whether any potential identifier, including a name, actually identifies an individual depends on the context.

By itself, the name ‘John Smith’ may not always be personal data because there are many individuals with that name. However, if the name is combined with other information (such as an address, school they





attend, or a telephone number) this is often sufficient to clearly identify one individual. "

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/#pd1>

Data Protection is all about making sure that personal information or data is kept secure and that individuals cannot be identified by anyone who isn't legitimately holding or processing information about a person.

IMPORTANT FACT: Personal information about a pupil is not just something in their personal school or Local Authority file. It is anything that identifies them. This can be informal or informal information. This includes emails or text messages and even notes.

Why Data Protection Is Important:

Data Protection is an important aspect of safeguarding as well as ensuring the privacy of individuals. Effective Data Protection is also the law, and it is there to protect us all. Key Principles for Data Protection:

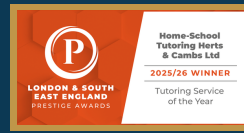
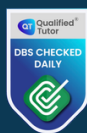
Watch this video created in Lockdown but is just as applicable now to tutors. The video is called 'Data Protection Advice to Teachers Working at Home':

<https://www.youtube.com/watch?v=yiPYZNVTYW8>

Key Principles from the video 'Data Protection Advice to Teachers Working at Home.' This is applicable to all Home-School Tutoring Tutors. This protects tutors and students:

- Make sure that your computer or laptop is fully up to date with any security updates and patches installed.
- Ensure you have appropriate anti-virus and anti-malware installed.
 - After this it is really a case of being careful about which websites you visit (checking for the padlock before the URL so that you know it is a secure site) and never open emails from unknown sources (if in doubt leave it alone).
- Teachers/Tutors must not share a device at home unless they are certain that no-one can access their data.
- Computers must be password protected and locked when not in use (so not accessible by anyone else without permission and pupil data locked down e.g. on a password protected data stick).

All school and Local Authorities have duties as public bodies to protect data. We all need to be aware that there is a corporate and personal risk and responsibility in handling data. We each have our own professional and personal responsibility for handling data correctly. It is vital we get it right. Not getting Data Protection Right is a serious reputation risk and there are also can be financial penalties on a





personal or organisational level:

"A new law came into force in the UK in May 2018, which outlines that employees can face prosecution for data protection breaches. As with previous legislation, the new law (the Data Protection Act 2018) contains provisions making certain disclosure of personal data a criminal offence. People have been prosecuted for misusing personal information obtained from their workplaces."

Don't let this make you anxious though. If we focus on prevention rather than cure in relation to 'Data Handling', we should be reassured that it is not complex to get Data Protection right. We all need to follow some simple guidelines.

Best Practice:

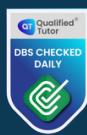
- Security starts with strong passwords. Make sure that you update your passwords regularly and that they are strong passwords. A strong password should include a mixture of uppercase and lowercase letters and a mixture of letters and numbers. It should also include at least one special character e.g. ! @ ? }
- Emails are the biggest risk for breached data because emails can be hacked, or they can go awry (often through human error). Never identify a pupil in an email or text message on a phone. For example, if the pupils is called Paul Smith use the initial P instead. We know our pupils, so don't need to be identifying them in any way. If you have a need to share data about a pupil, for example sending in a safeguarding referral, then you must encrypt this email using Egress Switch (or another encryption method). Please speak to your Area Advisor about Egress Switch or alternative means of sending sensitive data. Don't retain data you don't need. Delete old emails.
- Be very careful about who is copied into emails. To avoid copying in someone who shouldn't be seeing a specific email or information Do not 'reply all', if possible. Check what is further down an email trail. Start a new email conversation rather than reply to an old one including an email trail. Take care not to name people unnecessarily.
- If you are speaking about a pupil on the telephone, make sure that you cannot be overheard by anyone who is not authorised to know the information.

Personal Data Breaches:

If you are aware of a potential breach (e.g., sharing an email to a wrong email address). Please highlight this as soon as possible to your Area Advisor. Depending on what has been shared we may need to report it. The key thing is reporting a potential breach as soon as possible as this can be potentially contained and managed. This is one of the reasons why not using pupil personal identifiers in emails is so important (unless an encrypted email).

Subject Access Requests:

Schools and Local Authorities can receive a Subject Access Requests. This could include anything including





emails or text messages you have sent to them. Therefore, you must always assume that anything you write about a pupil could be released and could come under a Subject Access Request. Therefore, always be professional and never identify a pupil in an email or text message unless you need to, e.g., a safeguarding referral (which will be sent by Egress Switch). Always assume that the person you are writing about may one day read the message or email that you have sent. This could be the case if there is a Subject Access Request. If you need to have a sensitive or contentious conversation, then this is always best done by telephone rather than email.

Subject Access Requests: Any individual has the right to access their personal data and can make a Subject Access Request from an organisation. If a parent makes a SAR about their child at a school everything that has been written about the child (including information from anyone who has communicated with the school or Local Authority) must be provided to the parent. This necessitates sharing informal or formal information.

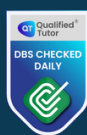
Freedom of Information Requests: This is not personal data, but information held by a school or Local Authority that people have a right to request.

Paper Records:

Paper records and notes are as important as electronic records in relation to Data Protection. Think before you print, and if you do need paper records or information about a pupil, they should not be accessible to anyone else except authorised individuals. So, paper records must be locked in a filing cabinet and must not be visible to family members if kept at home. Our recommendation to tutors is not to print anything about pupils at all unless completely necessary. In most cases printing personal information about a pupil is not necessary. If you need to take printed information to a meeting, you must be careful it is not left anywhere. Leaving personal information somewhere where someone else can find it is a breach of data protection and again can lead to fines or prosecution. Our recommendation is not to print sensitive or personal information about a tutee or to take it anywhere. Another thing to be aware of is notes in a diary or on other documents. Please avoid identifying pupils by their full names or date of births in personal diaries or other notes. Again, an initial should be enough in a diary. Unfiled notes like diaries are still covered by Data Protection Laws. If a diary is lost and contained personal information this is also a data breach and must be reported to your Area Advisor unless you are confident there are no personal identifiers contained in the personal paperwork. Therefore, our guidelines are that you don't use personal identifiers (full names) in any documents apart from encrypted emails.

Destroying Data:

You must destroy or hand over data or information as and when requested. E.g., when you stop working with a pupil. If you have paper records that need to be destroyed these must be shredded.





When it comes to data security for paper documents that you no longer need, there is no greater peace of mind than using a shredder to securely destroy them. Shred all obsolete paperwork to prevent confidential data falling into the wrong hands.

Data Protection for Tutors

Data Protection is not complex providing we focus on prevention, not cure, and are aware of our responsibilities. Home-School Tutoring has identified 4 Key Lines of Defence for All Tutors:

1. Devices fit for purpose:

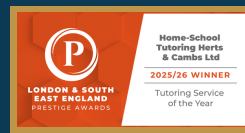
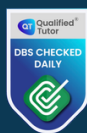
- Strong Passwords for all devices
- Computers must be password protected and locked when not in use.
- Data/memory USB sticks must be password protected.
- Ensure you have appropriate anti-virus and anti-malware installed.
- Make sure that your computer or laptop is fully up to date with any security updates and patches installed.
- Be careful about which websites you visit (checking for the padlock before the URL so that you know it is a secure site) and never open emails from unknown sources (if in doubt leave it alone).
- Tutors must not share a device at home unless they are certain that no-one can access their data (e.g., data locked down on a password protected data stick).
 - Encrypt messages (Egress Switch) when sharing data or important personal information about a pupil (e.g., safeguarding referral) with identifiers.

2. Identity markers avoided in all communication unless necessary:

- Never identify a pupil in an email or text message on a phone. e.g., if the pupils is called Paul Smith use the initial 'P' instead. We know our pupils, so don't need to be identifying them in any way. If you have a need to share data about a pupil e.g., sending in a safeguarding referral. Then, you must encrypt this email using Egress Switch or something similar. Please speak to your Area Advisor about Egress Switch or other ways of encrypting emails if you need to send sensitive data.

3. Be careful who you share information with:

- Be very careful about who is copied into emails. To avoid copying in someone who shouldn't be seeing a specific email or piece of information do not 'reply all', if possible.
- If you are speaking about a pupil on the telephone, make sure that you cannot be overheard by anyone who is not authorised to know the information
- You shouldn't share anything about a pupil without permission (except for safeguarding reasons to the right channels) and this is generally only if someone needs to know something about a pupil to do their job.
- Destroy all obsolete paperwork with a shredder so that it is not longer readable and shared with someone inadvertently.





4. Rapidly Report any issues:

➤ Data protection breaches must be reported speedily. This allows action to be taken to minimise the impact of a breach. Please contact your Area Advisor if you become aware of a data breach. They will take appropriate actions and seek advice where relevant. If it involves a school or Local Authority, then they will liaise with the appropriate person.

Date of Policy - September 2026

Date for Review - September 2027

