Edition 4

NEWSLETTER

The Data Protection Act 2018 has now been enacted, and is in force from 25 May 2018 - the same date as the General Data Protection Regulations (GDPR). As a Trust we have been working hard to achieve GDPR readiness and have the relevant core policies and procedures in place. It is now time to break down the key information from the new regulations and to continue to strengthen the safety and security of all data held in the Trust.

All staff have to play a part in GDPR compliance;

- you must know to speak to the DPO if you suspect a data breach, are undertaking a new form of data processing, or if a person makes a subject access request.
- be aware of the data you process - this can involve collecting, editing, retrieving, storing, archiving, disclosing and destroying either electronic or hard copies.

Think of it as similar to the relationship between staff and the designated safeguarding lead in this respect.

Staff Awareness / Training

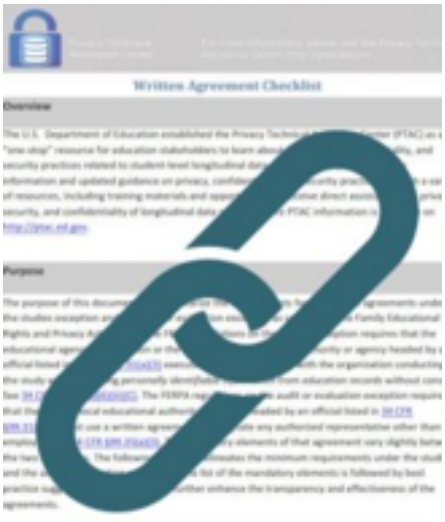
Please watch the GDPR training video and complete the quiz if you have not already done so. For any new members of staff, if you have not received your user name and password, then please contact dpare@evolvetrust.org with immediate effect. If you have your details then please watch the video and complete the quiz as a matter of urgency. **This is a mandatory requirement.**

Data Protection Policies

Please would you ensure you read the updated policies which are saved on the GDPR system as a matter of urgency. **This is a mandatory requirement.**

Here is the link to the training video and policies: GDPR.co.uk

Data Sharing Agreements



If there is a risk to sharing data with an organisation, we must have a data sharing agreement in place.

A data sharing agreement sets out a "common set of rules to be adopted by the various organisations involved in a data sharing operation".

There has been a great deal of work undertaken by the members of the GDPR Operations Team to ensure all contracts we have with organisations are GDPR compliant, and that where necessary addendum / data sharing agreements are in place.

If you are sharing special category data, you may decide to have one in place due to the sensitivity of the data. A data sharing agreement is an appropriate safeguard to have in place.

Agreements should be bespoke and should address; the purpose of data sharing, the organisations involved in data sharing, data items to be shared, basis for sharing, access and individuals' rights and information governance. All data sharing agreements must be reviewed regularly.

For further guidance on data sharing agreements, please email Dawn Pare, DPO on dpare@evolvetrust.org.

More on Subject Access Requests:

The previous GDPR Newsletter gave you information on SARs, however I wanted to share some further clarification with you.

The GDPR does not specify how to make a valid subject access request. Therefore, an individual can make a subject access request to you verbally or in writing. It can also be made to any part of the Trust (including via social media) and does not have to be to a specific person or contact point.

A request does not have to include the phrase 'subject access request' as long as it is clear that the individual is asking for their own personal data.

The challenge presented here is that any member of staff could receive a valid request.

The timescale for responding to a SAR is 30 days, therefore if staff receive a subject access request they must immediately forward it to the Data Protection Officer (dpare@evolvetrust.org)

GDPR Mythbuster

Myth	Fact
You need to seek consent for all the personal data you process.	You probably won't need to seek consent that often. You need to have a 'lawful basis' (legal reason) for processing personal data, and consent is just 1 of 6 lawful bases you can use. Only use consent where none of the other bases apply, as the standard for consent is very high and individuals can say no and withdraw it at any time.
You cannot ask visitors to sign in by putting their details into a visitor system.	It is clear that you need to keep certain visitor data for health and safety reasons. It is appropriate to capture and store the data you need to meet your legal obligations to keep staff and pupils safe.
Regarding data retention, it is enough to just delete the data from time to time	Implementing the "right to be forgotten" correctly is more complex than that. Previous law also recognised the concept of not storing data for longer than necessary. However, for the first time it explicitly states that the time period must be explicitly determined. This isn't a case of "one size fits all". Please follow the Trust's Information and Records Retention policy.
GDPR does not apply to paper	GDPR is technology-neutral; it doesn't matter whether you record data of subjects via an app or a paper logbook form. Any kind of processing of a structured and consistent set of personal data qualifies to fall under the scope of GDPR. It is fine to keep paper records, as long as you store and use them according to the GDPR principles for data processing.
You need to look at how you handle ALL the data you keep in school.	The GDPR only applies to personal data, which is any information relating to an identified, or identifiable, person. This may include information such as the person's name, contact details, unique identification number (such as National Insurance number or online identifier (such as username). It may also include anything relating to the person's physical and mental health, genetics, finances, or their physiological, cultural, or social identity. You don't need to worry about how you handle any data that can't be specifically linked to an individual - including data that has been anonymised.

Look out for Edition 5

for more guidance around The General Data Protection Regulation (GDPR)