# THE GENERAL DATA PROTECTION REGULATION (GDPR)

March 2018

## WHAT DOES IT MEAN FOR YOU ?

WRITTEN BY
LUCILE DE CARBONNIERES
DATA PROTECTION OFFICER

return 2 play

# General Data Protection Regulation

**The world has changed significantly since the Data Protection Act (DPA) was introduced in 1998. We now live in a very different environment for data where schools routinely communicate with parents, staff and pupils using a myriad of electronic means (emails, text, Twitter, Facebook, Instagram, etc.). Our data landscape has clearly been transformed beyond recognition and the rules required to police it needed an overhaul. So, what is the General Data Protection Regulation (GDPR)?**

# What is GDPR?

On the 25th May 2018 the current Data Protection Act (DPA) will be replaced by the new and updated General Data Protection Regulation (GDPR).

The purpose of the new regulation is to strengthen and unify data protection for all individuals within the EU, meaning that the way we manage all information and data will change.

The GDPR does a few things:

- It defines what is meant by 'personal data'
- It confers rights on 'data subjects'
- It places obligations on 'data controllers' and 'data processors'
- It creates principles relating to the processing of personal data
- It provides for penalties for failure to comply with the above.

Please note that these new rules apply to all personal data being processed, including using computers but also any kind of filing system with hard copies including paper.

## Main Differences between the GDPR and the DPA

The GDPR uses 6 "principles" (down from 8) and schools (Data Controllers) must comply with these and evidence how they do so. The principles are that data must be:

1. Processed fairly, lawfully and in a transparent manner
2. Used for specified, explicit and legitimate purposes
3. Used in a way that is adequate, relevant and limited to what is necessary in relation to the purpose sought
4. Accurate and kept up-to-date
5. Kept no longer than is necessary

6. Processed in a manner that ensures appropriate security of the data (Technical and organisational measures are put in place to protect the data from unlawful processing, accidental loss or destruction.

Companies in breach of the GDPR will face fines.

# What does it mean for you?

Under current legislation you already have a duty of care to ensure your data is kept safe and secure. And with the GDPR coming into effect you will have an increased responsibility to ensure this information – regardless of what form it is kept in – is managed in the right way in compliance with this new regulation.

## How to prepare

The Information Commissioner's Office (ICO) have put together a guide on Preparing for the General Data Protection Regulation (GDPR). You should keep checking the ICO website for further advice and support to help you prepare. Here are some of the steps they suggest your school should consider taking.

**Awareness**

- Ensure that key people in your school are aware that the DPA is changing to the GDPR
- Designate a Data Protection Officer to take responsibility for data protection compliance

**Consider what data the school holds and what it does with that data**

- Conduct a review of what personal data your school currently holds
- Consider and record for what purposes your school processes personal data, where it comes from and with whom it is shared
- Review the legal basis on which your school is entitled to process the personal data held. For example, has your school obtained parental/staff consent, or is the processing necessary for the school to comply with its legal obligations? Different justifications will exist for different types of personal data and processing activity
- Note that children under 13 years cannot 'consent' to the processing of their personal data'; consent can only be given by the holder of personal responsibility over the child.

**Review existing procedures**

- Review how your school currently seeks, obtains and records personal data and individuals' consent to the processing of their data, e.g. acceptance forms, parental consent forms etc. Under the GDPR all consent must be "freely given." This means that it must be a positive and unambiguous indication of agreement, not an agreement inferred from silence, inactivity, or pre-ticked boxes.
- At what stages do individuals have the opportunity to read and/or agree to privacy notices and privacy policies? On your school's website, hard copy, email?
- Consider whether your school's privacy notices and privacy policies contain all the necessary information that needs to be communicated to staff, parents and children?
- Is your school equipped to identify when a data protection breach has occurred? What is the process for investigating and remedying any such breach?

**Assess how your school deals with individuals exercising their rights**

- Does your school have adequate systems in place to correct or erase data at an individual's request?
- Assess the procedure for responding to a subject access request and whether this can be done within the GDPR's 30 calendar day timeframe
- Cease charging individuals when they make a subject access request
- Consent must also be able to be withdrawn at any time. In response, schools should look to review their parental contracts, acceptance forms, consent forms, etc.

**Identify areas of risk**

- Identify which areas of non-compliance are of the highest priority to address
- Put together a plan of action to remedy those areas of non-compliance
- What security measures does your school currently take in respect of personal data? Consider:
    - Are hard copies locked away or left on desks? Who has access to data that is locked away in filing cabinets, etc.?
    - Are electronic copies of data protected by strong passwords? If so, how many people know the passwords or would be able to find out the password?
    - Does your school store data on memory sticks? Do you keep your devices locked away when not in use?
    - Have firewalls and antivirus software been installed?

**Implement change (if needed)**

# What does it mean for your relationship with R2P?

GDPR demands a formal contract between the Data Controller (you) and the Data Processor (Return2Play), including how data is stored and processed. As a Data Controller, it is your responsibility to ensure third party suppliers that process data for the school, deemed Data Processors, also comply with GDPR.

Return2Play, as your Data Processor, is acting on behalf of your school to help protect personal data. We will ensure that there is a legally binding contract (or Third Party Data Sharing Agreement) in place to determine the formal processes involved and ensure that all of these processes are fully GDPR compliant.

We will set out, in our legal contract with you, our obligations which ensure that we:

- Process the personal data only on documented instructions from you, the Data Controller
- Ensure all staff involved in processing your data observe confidentiality
- Take all appropriate, and compliant security measures to protect your data
- Help you, the Data Controller, by using appropriate technical and organisational measures
- Help you, the Data Controller to ensure compliance
- Return or delete all the data at the end of the contract
- Provide the Data Controller with all information necessary to demonstrate compliance.

Return2Play will help you ensure the ongoing confidentiality, integrity, availability and resilience of your processing systems and services for your injury management system.

There seems to be a lot of anxieties related to the introduction of the GDPR however, we remain confident at Return2Play that schools are much better placed to address the new regulations than companies in other sectors.

Return2Play is a suitable partner who can help you manage your data in a safe, secure and compliant way, with correct policies and procedures in place.

# Annex 1: GDPR Checklist

**Data you hold**

- Have a list of all Personal Data you hold (often referred to as a Data Map) and:
    - the sources of that Data – where did you get the Data from
    - what was the reason for obtaining the Data
    - who you share it with
    - what you do with it
    - how long you keep it
    - how secure is the Data
- Have a list of places where you keep Personal Data and the Data exchanges between those places (databases, paper forms, etc.).
- Have a Privacy Policy, publicly accessible, where you explain all processes relevant to Personal Data (Records of Processing Activity).

**Data Management**

- Appoint a Data Protection Officer (DPO)
- Create awareness about GDPR guidelines
- Review your Data security (transfers, passwords, encryption, etc.)
- Train staff appropriately on data protection
- Have a contract in place with all of your Data Processors
- Have data breach policies and procedures in place

**New Data Subjects Rights**

- Make sure your Data Subjects can easily access their Personal Data
- Make sure your Data Subjects can easily update their Personal Data
- Make sure your Data Subjects can easily request the deletion of their Personal Data (unless you are required by law to keep it)

**Consent**

- Your Privacy Policy should be written in clear and understandable language
- Make sure Consent is "freely given".
- Make sure Consent can be withdrawn at any time.

**Follow-up**

- Regularly review policies and procedures.


return 2 play