



PAIGNTON RUGBY FOOTBALL CLUB LTD.

Founded as a Rugby Football Club in 1873 (Affiliated to R.F.U & D.R.F.U)

Queens Park, Queens Road. Paignton. Devon. TQ4 6AH

Telephone: 01803 557715 - Email info@paigntonrugby.com

www.paigntonrugby.com

Data Protection

What does GDPR actually do?

- ▲ 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

What is the difference between the DPA 2018 and the GDPR?

The GDPR is enacted in law in the UK by a new Data Protection Act which was granted Royal Assent on 23 May 2018. The UK's third generation of data protection law will commence on 25 May 2018.

The GDPR has direct effect across all EU member states and has already been passed. This means that organisations will still have to comply with this regulation and we will still have to look to the GDPR for most legal obligations. However, the GDPR gives member states limited opportunities to make provisions for how it applies in their country. One element of the DPA 2018 is the details of these. It is therefore important the GDPR and the DPA 2018 are read side by side.

What is 'personal data'?

"Any information relating to **an identified or identifiable natural person** (data subject); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person."

What is 'special category' data?

GDPR has also extended the definition of 'sensitive personal data' which requires even more protection than 'personal data.' 'Special category' data includes data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life or sexual orientation.

What rights do data subjects have under GDPR?

- ▲ The right to be informed
- ▲ The right of access
- ▲ The right of rectification
- ▲ The right to erasure



PAIGNTON RUGBY FOOTBALL CLUB LTD.

Founded as a Rugby Football Club in 1873 (Affiliated to R.F.U & D.R.F.U)

Queens Park, Queens Road. Paignton. Devon. TQ4 6AH

Telephone: 01803 557715 - Email info@paigntonrugby.com

www.paigntonrugby.com

- ▲ The right to restrict processing
- ▲ The right to data portability
- ▲ The right to object
- ▲ Rights in relation to automated decision making

What are 'data controllers' and 'data processors' under GDPR?

- ▲ The **Data Controller** is the person or organisation which determines the purposes and means of the processing of personal data: *Paignton Rugby Football Club becomes a data controller under GDPR.*
- ▲ The **Data Processor** is the person or organisation which processes the personal data on behalf of the controller. e.g. MIS provider, cashless catering supplier, library system supplier, or any other third-party supplier that uses personal data to provide the club with services or products

What obligations do Data Controllers have?

GDPR stipulates that the data controller shall "be responsible for, **and be able to demonstrate**, compliance with the principles."

The 'Six Principles' of GDPR

Personal data must be:

- ▲ Processed fairly, lawfully and in a transparent manner
- ▲ Used for specific, explicit and legitimate purposes
- ▲ Used in a way that is adequate, relevant and limited
- ▲ Accurate and kept up-to-date
- ▲ Kept no longer than is necessary
- ▲ Processed in a manner that ensures appropriate security of the data

To comply with GDPR, Data Controllers have to determine:

- ▲ The legal basis for collecting data
- ▲ Which items of personal data to collect
- ▲ The purpose(s) the data is to be used for
- ▲ Which individuals to collect data about
- ▲ Whether to disclose the data and, if so, to whom
- ▲ Whether subject access and other individuals' rights apply
- ▲ How long to retain the data



PAIGNTON RUGBY FOOTBALL CLUB LTD.

Founded as a Rugby Football Club in 1873 (Affiliated to R.F.U & D.R.F.U)

Queens Park, Queens Road. Paignton. Devon. TQ4 6AH

Telephone: 01803 557715 - Email info@paigntonrugby.com

www.paigntonrugby.com

What obligations do Data Processors have?

Data processors have obligations which **must be set out in a legal contract**.

Under GDPR, clubs and individuals within clubs can no longer merely sign a supplier's order form. There must be a legally binding contract in place that stipulates how the processor will meet their obligations under GDPR or we are not legally allowed to use that processor. This applies to existing, as well as new, suppliers that use personal data from the club.

Key changes affecting clubs;

a. The need to identify and record the legal basis for processing data before it is processed

- ▲ Before any personal data is processed, the data controller has to identify what legal basis they are using to process the data and **ensure this is recorded**.
- ▲ There are **six** legal bases that a data controller can consider and record.
 - ▲ Consent has been obtained from the data subject
 - ▲ Necessary for the performance of a contract with the data subject
 - ▲ Necessary for compliance with a legal obligation
 - ▲ Necessary to protect the vital interests of a data subject or another person
 - ▲ Necessary to carry out tasks in the public interest
 - ▲ Necessary for the purposes of legitimate interests pursued by the data controller or a third party

b. Consent conditions have been strengthened considerably

If the legal basis used is consent, this brings in a host of additional rules and requirements that could cause issues in clubs;

- ▲ Consent must be freely given
- ▲ Consent must be specific
- ▲ Consent has to be in the form of a clear, affirmative action
- ▲ Consent has to be separate from any other terms and conditions
- ▲ Consent can be withdrawn at any time
- ▲ Consent needs to be verifiable

In addition, the new Data Protection Act sets the age of (data) consent for data processing at 13 in the UK.

c. Data breaches must be notified to the ICO within 72 hours

Under the DPA (1998), notification of data breaches was voluntary, rather than mandatory. This is not the case under GDPR.



PAIGNTON RUGBY FOOTBALL CLUB LTD.

Founded as a Rugby Football Club in 1873 (Affiliated to R.F.U & D.R.F.U)

Queens Park, Queens Road. Paignton. Devon. TQ4 6AH

Telephone: 01803 557715 - Email info@paigntonrugby.com

www.paigntonrugby.com

Under GDPR, all data breaches which have the **potential** to have a significant detrimental effect on the individual(s) through discrimination, damage to reputation, financial loss, loss of confidentiality or any other economic or social disadvantage must be reported by the data controller to the ICO within 72 hours of discovery.

d. Individuals have an increased right of access to their data and its use

All individuals will have a right to obtain confirmation that the Data Controller is processing their personal data in line with GDPR.

They will be able to demand access to **all** their personal data we are processing including **what** data we are processing, **why** we are processing it, **who** it is being shared with, **how long** it is being retained, etc.

e. Under GDPR, individuals will have the 'right to be forgotten'

Where the personal data is no longer required for its original purpose, their consent has been withdrawn, **or** they object to the processing, an individual can demand that the processing is stopped and all their personal data is erased by the data controller, including from any processors the controller has shared this data with.

f. GDPR requires data controllers to be accountable for the personal data they process

This means that not only do we **all** have to comply with GDPR, we have to be able to **evidence** this, too, by keeping accurate records of processing and undertake regular and documented monitoring and audits.

There are substantial implications for staff training. Just like with Safeguarding, we will be required to undertake regular whole staff training around data protection and keep records of this training.

g. 'Privacy by design' becomes a legal requirement under GDPR

Privacy by design means ensuring that the protection of any personal data is considered at the very outset of any new processes or technologies that we intend to implement, rather than it being something that is thought about at a later stage.

It will mean staff training to evidence that they have been taught about this and how to undertake Privacy Impact Assessments (also known as Data Protection Impact Assessments – DPIAs).

h. Data protection officers need to be appointed

The DPO has three main responsibilities:

- ▲ To advise and inform the club about their obligations to comply with GDPR and any other data protection legislation
- ▲ To monitor the club's compliance with GDPR conduct audits, etc.
- ▲ To be the first point of contact with the ICO and data subjects



PAIGNTON RUGBY FOOTBALL CLUB LTD.

Founded as a Rugby Football Club in 1873 (Affiliated to R.F.U & D.R.F.U)

Queens Park, Queens Road. Paignton. Devon. TQ4 6AH

Telephone: 01803 557715 - Email info@paigntonrugby.com

www.paigntonrugby.com

GDPR states that the DPO must:

- ▲ Report to the highest level of management
- ▲ **Be independent**
- ▲ Not be penalised for doing their job
- ▲ Be provided with adequate resources to perform their tasks
- ▲ Have professional experience and knowledge of GDPR and data protection law
- ▲ Have no conflict of interest

“Achieving compliance will require unconditional support from all staff: PAYE & Volunteers

Data protection needs to become as ingrained in our day-to-day working as safeguarding.”



PAIGNTON RUGBY FOOTBALL CLUB LTD.

Founded as a Rugby Football Club in 1873 (Affiliated to R.F.U & D.R.F.U)

Queens Park, Queens Road. Paignton. Devon. TQ4 6AH

Telephone: 01803 557715 - Email info@paigntonrugby.com

www.paigntonrugby.com

What do we need to do?	How will we do this?	What progress have we made?
Raise awareness	a. Raise awareness across all staff within the College who come into contact with personal data (noting that personal data can relate to students, staff, parents and, potentially, others).	
	b. Ensure that a broad range of staff across the College community are engaged with the work both to articulate and demonstrate the totality of personal data owned by the College and to be engaged in risk management.	
	c. Ensure that Governors are aware of the key issues arising for the College from the legislative changes and understand how to effectively monitor and review compliance with the data protection regulations.	
	d. De-mystify the language associated with data protection, and the enhanced legislation.	
Create a 'high level' data map	a. Build up an initial overview of all the places personal data are stored and used in the College (the College's 'data eco-system').	
	b. Create something that can be discussed and tested with staff to identify any gaps in the initial overview and build confidence that everything is captured.	



PAIGNTON RUGBY FOOTBALL CLUB LTD.

Founded as a Rugby Football Club in 1873 (Affiliated to R.F.U & D.R.F.U)

Queens Park, Queens Road. Paignton. Devon. TQ4 6AH

Telephone: 01803 557715 - Email info@paigntonrugby.com

www.paigntonrugby.com

	c. Create an overview that can be aligned to more detailed documentation about data assets.	
--	---	--



PAIGNTON RUGBY FOOTBALL CLUB LTD.

Founded as a Rugby Football Club in 1873 (Affiliated to R.F.U & D.R.F.U)

Queens Park, Queens Road. Paignton. Devon. TQ4 6AH

Telephone: 01803 557715 - Email info@paigntonrugby.com

www.paigntonrugby.com

Turn our data map into a data asset register	a. Create the main framework around which we can document the detail associated with each dataset.	
	b. Identify the areas of weakness/risk or gaps that will most likely begin the creation of a risk-management based approach to compliance.	
Document the reasons for processing data	a. Become familiar with the conditions and lawful basis for processing that are most relevant to the activity of schools.	
	b. Understand the extra conditions and compliance that is required to process special categories of data and criminal offence data.	
	c. Understand that lawful bases are specific to processing data: the purpose that we are using it for.	
	d. Identify the processing activities that do not appear to be essential to undertake the task of safely and efficiently running a school. These are the areas that informed specific consent from data subjects may need to be sought if not already obtained.	
Document how long we need to retain information	a. Create a workable data retention policy that can be discussed and iterated with those who best understand your uses of data.	



PAIGNTON RUGBY FOOTBALL CLUB LTD.

Founded as a Rugby Football Club in 1873 (Affiliated to R.F.U & D.R.F.U)

Queens Park, Queens Road. Paignton. Devon. TQ4 6AH

Telephone: 01803 557715 - Email info@paigntonrugby.com

www.paigntonrugby.com

	b. Understand that data retention is based on justification: if we can justify it, we can keep it.	
--	--	--



PAIGNTON RUGBY FOOTBALL CLUB LTD.

Founded as a Rugby Football Club in 1873 (Affiliated to R.F.U & D.R.F.U)

Queens Park, Queens Road. Paignton. Devon. TQ4 6AH

Telephone: 01803 557715 - Email info@paigntonrugby.com

www.paigntonrugby.com

Identify and mitigate risks	a. Identify risks which emerge from the initial completion of our data asset register.	
	b. Assess what can be done to eliminate or reduce areas of medium/high risk and set action plans to do so.	
	c. Use Data Protection Impact Assessments as part of our risk identification and mitigation procedures.	
	d. Ensure that we have up to date data sharing agreements with 3 rd party processors (organisations with whom we share data).	
Appoint a Data Protection Officer (DPO)	a. Understand the role of the DPO and be clear that each school needs to appoint a DPO in order to be compliant with new legislation.	
	b. Understand the different options for appointing a DPO so that we can decide what is the best value and most effective solution for us.	
	c. Appoint DPO and communicate this to ICO and data subjects.	



PAIGNTON RUGBY FOOTBALL CLUB LTD.

Founded as a Rugby Football Club in 1873 (Affiliated to R.F.U & D.R.F.U)

Queens Park, Queens Road. Paignton. Devon. TQ4 6AH

Telephone: 01803 557715 - Email info@paigntonrugby.com

www.paigntonrugby.com

Communicate with data subjects	a. Be familiar with the full potential rights data subject has and the circumstances in which these do not apply: exemptions exist.	
	b. Consider how best to demonstrate our compliance with new legislation. This is a key focus of what is changing. Compliance alone is not enough.	
	c. Update our Privacy Notices and communicate these to staff, students and parents.	
	d. Understand the benefits of being open and transparent with data subjects. There is more to building trust than compliance alone.	
	e. Understand the key changes to Subject Access Requests and put procedures in place for handling these.	
‘Operationalise’ data protection and ‘keep it living’	a. Identify the range of policies required within the College that cover the procedures and processes for data protection. Ensure that all policies are reviewed, reworked and readopted (as required).	
	b. Understand what constitutes a data breach and what to do about it.	



PAIGNTON RUGBY FOOTBALL CLUB LTD.

Founded as a Rugby Football Club in 1873 (Affiliated to R.F.U & D.R.F.U)

Queens Park, Queens Road. Paignton. Devon. TQ4 6AH

Telephone: 01803 557715 - Email info@paigntonrugby.com

www.paigntonrugby.com

	c. Ensure that data protection and risk management is a core and regular part of decision making and risk management practices within the College.	
--	--	--