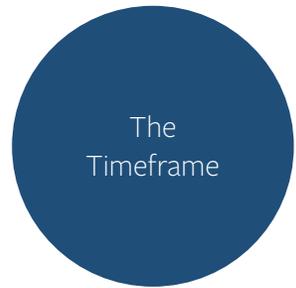


General Data Protection Regulation

What your school leadership needs to know



The
Timeframe

GDPR becomes law on
25th May 2018

It comprises of:
99 'articles'
173 'recitals'



Effects personal
data of all EU
citizens

Replaces existing data
protection laws in every
EU country with one
harmonious regulation.

Applies to **any** organisation
in the world that processes
EU citizens personal data.



Ramifications of
non compliance

Fines up to €20 million or 4%
of annual revenue.

Enforcement will be pro-active
though fines are a last resort.



Appoint a GDPR
Champion

Appoint someone to lead
the project and understand
what the GDPR is.

Do not underestimate the
time commitment.



Starting point:
Review, audit &
report

Start by understanding the
scope of work required.

It could be weeks or
months depending on the
size of your school and
how advanced your data
management is.



Plan & provision
for resources
and time

With a review or audit,
develop a plan and
adequate resources to
reach full compliance
before May 2018.



NEW
Appointment
Data Protection
Officer

Requirement to appoint a
Data Protection Officer.

DPO duties can be given to
an existing member of staff
or contracted in.

12 steps to take now:

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

5 Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7 Consent

You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8 Children

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11 Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.