Pocklington Community Junior School
65 Kirkland Street, Pocklington, York YO42 2BX
Telephone: 01759 302224
Email: admin@pocklingtonjuniors.co.uk

www.pocklingtonjuniors.co.uk

GDPR – Q&A

(please note that any reference to GDPR may be subject to change as the Data Protection Bill progresses)

What is GDPR and how does it affect me?
GDPR stands for General Data Protection Regulation. It is a European wide piece of legislation that will be enforced across all EU Member States from 25 May 2018.

The regulation replaces the Data Protection Act 1998 which is now very out of date.

Generally the principles of the Data Protection Act 1998 migrate over to new legislation. Many of the new requirements have been best practice for a number of years. This means that it is likely that you will not see a lot of change to your day to day work.

What is the Data Protection Bill?
As well as the GDPR the UK requires a second piece of legislation to ensure that (a) GDPR is enforced across the Country and (b) to fill in the gaps where the UK can decide its own laws (e.g. law enforcement and age of consent for social media accounts).

When the Bill is approved by Parliament it will become the Data Protection Act 2018.

Do we need to have consent every time we use somebody's information?
No. This is a common misconception. The Trust and its schools should only be relying on consent, as a reason to use personal data, when it wants to offer genuine choice. In most cases the Trust will be relying on its legal powers or authority to use personal data. Consent must only be used if it is just as easy to withdraw is it is to give. As a Trust we generally tell people how we use their personal data rather than asking for consent.

For example it would be suitable to ask for consent if you want to send a newsletter to a parent. It would not be suitable to ask for consent to use personal data to forward it to an outside agency (without explicit consent).

Do members of the public really have a 'Right to Be Forgotten'?
The GDPR does offer individuals a right to ask organisations to erase all data that it holds about them.

However, this is only really likely to be approved if:

- The organisation has relied on consent to collect that person's personal data,
- The organisation no longer needs that data for the purpose it was collected,

Everybody has a right to ask for their data to be erased but generally the Trust will reject such requests when it has relied on a legal power or authority to use somebody's personal data.

What should I do if I receive a Data Protection Request?
As well as 'the Right to be Forgotten' a service user may also exercise other Data Protection requests:

- Right to Correction
- Right of Access (Subject Access Request)
- Right to Restriction

- Right to prevent automated decision making

A service user may submit a request to any member of staff in the Trust. It is therefore important that you know what to do if you receive such a request.

Please, in the first instance, refer all such requests to the Head of Operations and Administration who will seek advice from the DPO.

What is an Information Security Incident and what should I do if I discover one?
An information security incident, commonly known as a Data Breach, is when personal data is accidently or purposefully lost, corrupted, or destroyed.

It is crucial that if you discover an information security incident, no matter how small, that you report it to the Head of Operations and Administration or Headteacher immediately. You should also attempt to retrieve the data as soon as possible. **It is vital that you note: any data breach needs to be reported to the ICO within 72 hours. If this is during term-time, weekends, or holidays – it makes no difference. Emergency contact details will be provided by each school within the Trust to its staff, to enable any breaches to be reported.**

To ensure that data breaches are kept to a minimum, staff should be aware that the safest way to work is on the school server; whether this is in school or at home. All documents and information kept within the school servers are secure and comply with GDPR. Information and documents should not be saved to personal devices or cloud-based applications.

Please see the Trust Policy for more information.

How much could the school be fined for a data breach?
Under the new legislation an organisation could be fined up to £17million *or* 4% of annual turnover (whichever is higher). This is an increase from £500,000 which is the current penalty limit.

It is important to note that fines are only issued as a last resort where there has been a series of serious data protection breaches.

Fines are also issued proportionately meaning that the likes of Google, Microsoft, and Facebook could be issued with a multi-million pound fine but it is unlikely that a Public Authority or school will ever be fined over a million pounds for a data protection breach.

Will I be trained on the new legislation?
Staff will initially be briefed by Head of Operations and Administration
The Trust's Data Protection Officer will deliver formal training sessions at the start of the new academic year. These sessions will give a brief overview of the changes under GDPR following staff briefing/information training sessions throughout Trust schools in May 2018.

More in depth training will be given for those with specific responsibilities – such as Information Asset Owners.

Further guidance will also be issued on approval of the Bill.

What is an information asset register?
An Information Asset Register (IAR) is a simple way to help the Trust understand and manage its information assets and the risks to them.

An information asset is a body of knowledge that is organised and managed as a single entity. An example would be the names of all pupils on roll or the data we hold in SIMS.

It is important for us to know and fully understand what information we hold in order to protect it and be able to exploit its potential.

We have updated the Trust's IAR. Once updated we will make a copy available to colleagues.

What is an information asset owner?
Each asset should have an Information Asset Owner (IAO). This is the officer – usually a manager or team leader - responsible for ensuring that the risks to, and the opportunities for, the asset are monitored.

The IAO doesn't need to be the creator or the primary user of the asset, but they must understand its value to the organisation. See also the Cabinet Office's Guidance on IAOs:
https://www.gov.uk/government/publications/information-asset-owner-role-guidance

If you have any Data Protection Concerns then please contact the Head of Operations and Administration or Data Protection Officer at: schoolsDPO@veritau.co.uk