GUIDE TO THE GDPR

SO, WHAT'S IT ALL ABOUT?

The General Data Protection Regulation (GDPR) came into force on 25th May 2018 and brought changes to existing Data Protection legislation. If you were already complying with current Data Protection legislation then it won't mean a great deal of change for you. The legislation gives greater rights and protections to individuals and brings consistency to legislation throughout Europe.

DEFINITIONS:

Personal Data - It's all related to information which can identify a natural person – this is called personal data. So if you hold information which can identify a living individual or you can add some information to what you hold and identify a living individual then that's covered by GDPR. So don't just think names and addresses but unique ID numbers and mobile phone numbers, for example.

SPECIAL CATEGORIES ALSO KNOWN AS SENSITIVE PERSONAL DATA:
See categories below:-

a. Racial or ethnic origin of the data subject;
b. Political opinions;
c. Religious beliefs or other beliefs of a similar nature;
d. Member of a trade union;
e. Physical or mental health or condition;
f. Sexual life;
g. Commission or alleged commission by him of any offence; or
h. Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

THE GDPR PRINCIPLES:

GDPR is based around 6 principles and these are listed below:-

1. Personal information must be processed fairly, lawfully and in a transparent manner;
2. Personal information is collected for specified, explicit and legitimate purposes;
3. Personal information must be adequate, relevant and limited to what is necessary ('data minimisation');
4. Personal information must be accurate and, where necessary, kept up-to-date;
5. Personal information must be kept for no longer than is necessary;
6. Processed in a manner that ensures appropriate security of the personal data.

KEEPING PERSONAL DATA SAFE:

GDPR requires that sufficient technical and organisational measures are taken to keep personal information safe. This includes considerations in relation to hardware, software, policies and procedures and training.

SO, WHAT'S CHANGED?

Wider Definition of personal data - Introduction of the term 'concerning' in relation to health and sexuality; also the introduction of biometrics, genetics and location data for the first time.

Increased rights for individuals - The fee for subject access have been scrapped and individuals have a right to be told how their data is being processed and why.

Accountability – Data Controllers now need to evidence that they are complying with GDPR. This can be through publishing policies and procedures on their website and also keeping good accurate records.

Appointing a Data Protection Officer - Public bodies, including schools, must have a named DPO.

Data breach reporting - Within 72 hours any serious breaches need to be notified to the ICO.

Legal Basis to process and Consent - Organisations have either a legal basis to process or they must seek consent. Consent must be freely given and also can be freely taken away.

Children - If you are over 13 years of age and under 16 years of age, you require parental/carer consent to use Internet services. Children have increased rights to have their data erased.

Automated decision making/profiling - Individuals can have any automated decisions reviewed and object to profiling.

WHAT ABOUT RIGHTS?

There are specific rights under the legislation:-

The right to be **INFORMED;**

You have a right to be told HOW and WHY your data is being used, who it is being shared with, and if your fundamental rights or freedoms may be affected. You must also be told if your data was involved in a data breach.

The right of **ACCESS;**

From May 2018 each of us can request, AT NO CHARGE, a copy of our personal information, and it must be provided within 1 month after identity confirmed.

The right of **RECTIFICATION;**

Just the same as now, you have a right to demand that any data held on you which is inaccurate or incomplete is rectified.

The right to **ERASURE;**

Also known as 'the right to be forgotten', is your right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to **RESTRICT PROCESSING;**

When you ask for processing to be restricted, organisations are permitted to store the personal data, but not further process it. They can retain just enough information to ensure that the restriction is respected in the future.

The right to **DATA PORTABILITY;**

Gives you the right to move your personal data, held in an electronic format, for example, held on social media, from one IT environment to another.

The right to **OBJECT;**

You have an absolute right to object to your data being used for direct marketing, and qualified rights if your information is being used for research purposes or company's legitimate interest or public interest/exercise of official authority.

The right to object to **AUTOMATED DECISION MAKING AND PROFILING;**

You have a right to ask for any decision made on you which is made by a computer to be reviewed by a human being, and you can object to organisations profiling your behaviours and characteristics.

TELL ME ABOUT CONSENT:

Individuals now have more control over the information they receive and also more control over who can process their data. In practice, this means:-

- Individuals have more choice and more control;
- Consent has to be a positive opt in not an opt out or a ticked box as a default;
- In relation to sensitive personal data, this requires explicit consent;
- Consent forms need to be specific and not generic although several consent boxes can exist on one clear form;
- Consent must be as easy to take away as it was to give;
- Review your consent documentation and keep it valid.

Remember it's not all about consent, look to your legal basis for processing, such as educating and health and safety of students.

SECURITY MATTERS:

The GDPR places responsibilities on us to help keep personal data safe and secure and there are many ways to do this. Below is a list to get you thinking about how secure your organisation is, in relation to personal data. Your organisation should have:-

- A secure ICT network;
- Anti-virus software and up to date patches;
- Regular back-ups taken;
- Methods to dispose of digital devices securely;
- Firewalls;
- Access to encrypted email when needed;
- Methods of training staff and keeping them up to date regarding Data Protection compliance;

- Hierarchy access in place which only allows individuals with lawful reasons access to personal data;
- Audit trails of access to personal data;
- Relevant Data Sharing Agreements in place;
- Up to date Records Retention and Destruction policy;
- Clear Desk policy.

IN RELATION TO PERSONAL DATA, PLEASE DON'T:-

- Ignore your organisations' policies and procedures in relation to Data Protection;
- Share passwords with colleagues;
- Write passwords down and have them on open display;
- Use unencrypted USB sticks;
- Send e-mails via unsecure methods;
- Access information you have no legal right to see;
- Take information home/away from base and leave it unsecured;
- Leave confidential waste paper in an insecure location;
- Ignore security risks or breaches.

SHOULD I PANIC?

NO - It's not expected that you will have everything in place for 25th May 2018 but you need to demonstrate that you do have a plan moving forward. You will need evidence of policies and procedures which demonstrate your commitment to and compliance with GDPR.

Here are some of the things you should be doing/plan to do within the coming months and by the end of 2018:-

- Ensure you have a current notification with the ICO for your organisation;
- Publish Privacy Notices on your website;
- Have a Data Protection policy;
- Know what information you hold and process;
- Have a named Data Protection Officer;
- Have a current Records Retention and Destruction policy;
- Make sure paper records are securely destroyed and certificates obtained;
- Have contracts and data sharing agreements in place with data processors.

By having the above in place you will reduce your risks.

For additional help or advice contact – Jane Corrin, Data Protection Officer on 0151 666 4446 or e-mail Schoolsdpo@wirral.gov.uk