On the 25th May 2018, the General Data Protection Regulation (GDPR) will come into effect across all EU member states. The GDPR provides one framework data protection law for Europe, representing a significant harmonisation of data protection requirements and standards across the EU. Having just one horizontal framework law to deal with will benefit business, promote responsibility when dealing with personal data, and help ensure that the same data protection standards apply across the EU.
It is important for all schools and childcare facilities to be aware that they will be required to comply with the data protection standards and obligations set out in both the GDPR and the Irish Data Protection Act 2018.

If you process personal data as part of your operation then the GDPR applies to you.

It is important to remember that:

- Parent, Child, Staff and non-staff employee data is **personal data**
- Storing personal data electronically or in hardcopy constitutes **processing personal data**.

There are four key groups who manage the processing of personal data within the school.

1. **DATA CONTROLLER**
   Principal & Deputy Principal. They decide the purpose for which, and the means by which, personal data is processed. The purpose of processing data involves '**why**' the personal data is being processed and the '**means**' of the processing involves '**how**' the data is processed.

   The Data Controller also decides what constitutes personal data for the purpose of the regulation. e.g. Daily attendance records may not be considered 'Personal Data' and therefore would not require the same security as other data.

2. **DATA PROCESSOR**
   Teachers and Office Staff. They processes personal data on the behalf of the data controller.

3. **DATA SUBJECT**
   Child, Parent Teacher or non-teaching staff, is the individual the personal data relates to.

4. **DATA PROTECTION OFFICER**
   Person appointed by the school to understand and manage the GDPR process. This individual will conduct audits and ensure that the GDPR is being properly maintained within the school.

5. **3rd PARTY SUPPORT**
   External company or individual who manages IT within the school and who has access to the schools systems and confidential files. This company or individual can also hold the position of DPO. It's important that a confidentiality agreement is put in place between the school and any 3rd part who has access to the schools systems or files.

'When your school collects, stores or uses (i.e. processes) personal data, the individuals whose data you are processing may be exposed to risks. It is important that schools which process personal data take steps to ensure that the data is handled legally, securely, efficiently and effectively in order to deliver the best possible care.'

Paper Data Records

- To be held in secure rooms, cabinets or filing cabinets under lock and key
- Files should not be accessible when the area is unattended. Therefore filing room and cabinets should have the keys removed when the people responsible for the security of the files have left the area.

Digital Data

Data may be kept on a device with a reputable Internet Security program and encryption installed. In the event of unauthorised access by whatever means the data should be protected.

Unauthorised access can be through the device being left unattended, hacked or stolen (hard drive removed)

A decision must be made on the process and procedures that the school wants to use to secure the storage, access and use of personal data. This will determine how the school secures individual devices.

Steps to the successful implementation of GDPR

1. Install Internet Security on all devices that either use or hold personal data or are connected to the school network. This includes the school server, office PC, classroom PC/Laptop's, Teachers Laptop's, Computer Room devices, Tablets and Smart Phones.

2. Audit all devices used in the school to determine what personal data is currently stored on these devices.

3. Record the findings in a database designed to register all aspects of the GDPR. **GDPR***plus* is a database software program installed in the school and not in the cloud, which is specifically designed to administer the requirements of GDPR.

4. Choose the best option that meets the needs of the school

RYEPEG software systems

OPTION 1

- Install Internet Security on all devices that can connect to the schools network.
- Ensure that any staff member who use their own personal PC or Laptop have a reputable Internet Security program installed on their device. Free versions are not considered adequate.
- Install Encryption Software on all devices that will store, access or use personal data.
- Prohibit the use of 'free' cloud storage (Dropbox, Google Drive) for the transfer or storage of personal data.

This option is more complex and difficult to implement and maintain. If the device is damaged the data may not be retrievable.

This option is the most expensive to implement.

OPTION 2

- Install Internet Security on all devices that can connect to the schools network.
- Ensure that any staff member who use their own personal PC or Laptop have a reputable Internet Security program installed on their device. Free versions are not considered adequate.
- Install a Buffalo TeraStation NAS (Network Accessible Storage) or similar onto the schools network.
- Create a Public and Private folder structure for users on the NAS unit.
- Assign passwords for individual users in line with recommended standards.
- Prohibit the use of 'free' cloud storage (Dropbox, Google Drive) for the transfer or storage of personal data.
- Provide Encrypted USB Flash Drives for use on devices or transfer of data outside of the school

This option is the most cost effective and the easiest to install and maintain. The individual users devices are not encrypted so the users can have easier passwords for their PC's or Laptops. Data is only accessible via the TeraStation on the network. Users are prohibited from copying data from the NAS unit to their local device. Working off-site can only be done using the encrypted USB Flash Drive.
Passwords provided to access the NAS Drive are much stronger and should never be saved in order to making logging on more convenient for the user.

School Website

Posting information, and in particular photo's of children which is considered personal data, onto the schools website requires permission from parents or guardians in order to do so.

Permission is also required from staff if their images are also uploaded.

It is now necessary to consider whether consent was freely given and the data subject must have the opportunity to withdraw consent for processing at any time.

Consent should not be assumed and must be obtained before data processing begins (e.g. through Privacy Notices). When processing the data of children in the context of online services, it is necessary to ensure that their age is verified and the consent of a legal guardian must be obtained. In Ireland, the Government is proposing that the age of digital consent, below which parental consent will be necessary, will be thirteen.

Right to Erasure *(Right to be forgotten)*

Extract from Article 17 of the GDPR

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: *Click this link to view the grounds* https://gdpr-info.eu/art-17-gdpr/

The school should consider not uploading data to 3rd part applications such as YouTube as this may make the task of 'Erasure' both difficult and complicated if a request is received.

The school should consider not archiving previous years websites because data held in the archives would also have to be erased if a request is received

Website 'Cookie' Banner

Websites that record or store information as the result of a user accessing the site must have a pop-up banner that informs the users of this fact and gives them an option to continue on the site or to leave the site.

This link provides further information the type of which should be accessible by the user if they require such information

http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

Websites designed using Weebly and Wordpress save such information.

For further information please contact:
Gerry Poynton
RYEPEG Software Systems
086 6034728
gerry@ryepeg.ie
www.ryepeg.ie

RYEPEG
–software systems–