Data Protection

A new European Union-wide framework known as the General Data Protection Regulation (GDPR) came into force across the EU on 25 May 2018. ... They provide for higher standards of data protection for individuals and impose increased obligations on organisations that process personal data.

Those members of staff that have access to personal data must comply with the company data protection policy.

DATA PROTECTION BASICS

Data protection law covers most situations in which information about somebody (the 'personal data' of a 'data subject') is used in some way ('processed') by some other person or organisation (the 'controller'), other than in a purely personal context.
The Data Protection Commission (DPC) is responsible for regulating different sets of laws, which cover different ways and circumstances in which personal data might be processed. These laws are set out below and on the DPC's website.

The 'General Data Protection Regulation' (GDPR) is the law which applies to most kinds of processing of personal data and it applies directly in Ireland (and across the EU), along with further national rules set out in the Irish Data Protection Act 2018.
However, the GDPR does not apply to the processing of personal data by an individual for 'purely personal or household' activities, with no connection to a professional or commercial activity. This is sometimes known as the 'personal/household/domestic exemption'. This might cover activities such as correspondence, keeping an address book, or certain social networking, where these activities are purely personal. The GDPR would still apply to controllers who process personal data to facilitate these

activities (such as a social network).

Where processing takes place for law enforcement purposes (such as preventing or detecting crime) the GDPR does not apply, and instead the 'Law Enforcement Directive' (LED) covers these situations, the rules for which are found mainly in Part 5 of the Data Protection Act 2018 (which implements the LED into Irish law).

Ireland's 'ePrivacy Regulations' (S.I. 336/2011, which implemented the EU 'ePrivacy Directive') are an extra set of rules which apply to certain types of processing, including electronic direct marketing and cookies, and these rules apply in addition to the rules found in the Data Protection Act 2018 and the GDPR.

These laws set out various obligations on data controllers and rights for data subjects, some of which are discussed below. They also set out the powers and responsibilities of the DPC. If you have a concern that a controller has failed to follow the law or uphold your rights, the guidance below should help you (a) make a request to a controller, or (b) make a complaint to the DPC, if they fail to comply with your request or their obligations under data protection law.

Personal data basically means any information about a living person, where that person either is identified or could be identified. Personal data can cover various types of information, such as name, date of birth, email address, phone number, address, physical characteristics, or location data – once it is clear to whom that information relates, or it is reasonably possible to find out.

Personal data doesn't have to be in written form, it can also be information about what a data subject looks or sounds like, for example photos or audio or video. recordings, but data protection law only applies where that information is processed by 'automated means' (such as electronically) or as part of some other sort of filing system.

Personal data can be information where the data subject is identified.

Even where personal information is partially anonymised, or 'pseudonymised', but this could be reversed and the data subject could possibly be identified using

additional information, it should still be considered personal data. However, if information truly anonymised, irreversibly, and could not be traced back to an identified person, it is not considered personal data.
To determine whether a person is 'identifiable', particularly where the information about that person is pseudonymised, all the methods and information reasonably likely to be used by the controller or other person to identify someone, either directly or indirectly, have to be considered.

Certain types of sensitive personal data, called 'special categories', are subject to additional protection under the GDPR, and their processing is generally prohibited, except for where specific requirements are met (such as having explicit consent), as set out in detail in Article 9 GDPR. The special categories are: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data processed to uniquely identify a person; data concerning health; and data concerning a person's sex life or sexual orientation.

Data protection law governs situations where personal data are 'processed'. Processing basically means using personal data in any way, including; collecting, storing, retrieving, consulting, disclosing or sharing with someone else, erasing, or destroying personal data. Although, as mentioned above, data protection law does not apply where this is done for purely personal or household activities.

It is the duty and obligation of St Marys to strictly observe the current GDPR regulations and therefore data is limited to those members of staff that need access and those staff only. Compliance is mandatory and constantly reviewed.