GENERAL DATA PROTECTION REGULATION

European Directive – May 2018. Replaces DPA (1998), as IT changed so much.

Safeguards to protect an individual's data, such as who you are, address, etc.

Need to know what the data is being used for and how long it will be stored.

KEY PRINCIPLES OF GDPR

Must have legitimate reason to hold data and advise use of such.

Data can only be used for original purpose notified – if no notification given - cannot use data.

Data Controllers may only collect minimum of data needed for task.

Data must be accurate, checked and confirmed.

Retention policy required so stored data is held for limited period only – no archiving.

Data must be secure, whether physical/cloud/or electronic, including 3rd party contractors.

DATA

Information that relates to a living person which identifies them and includes opinions. Sensitive information – Racial/ethnic origin, religious beliefs/political opinions/unions/health/sexual orientation/genetic and biometric data.

DATA SUBJECT

Person whose details are kept on file – Inform how data is held and have right to access (limited say re child protection/legal/contract exceptions) Subject can request old data to be amended/deleted. Any legal proceedings data must be preserved.

DATA CONTROLLER

The organisation ultimately responsible for data collected about data subject.

DATA PROCESSOR

Person/organisation that uses collects or amends the data on behalf of data controller. Could be member of staff/temp/3rd party company/contractor/or organisations such as police or LA. Data controllers in charge to check data processor is as careful about data as themselves.

PROCESSING DATA

Have consent of data subject

Necessary for performance of a contract

Necessary to comply re legal obligation

To protect vital interest of data subject or another person

Necessary for task to be carried out in public interest or for official authority

Legitimate interests by controller or 3rd party (but not where data subjects' rights override controller)

DATA PROTECTION OFFICER

Every public authority must have one.

Informs controller/processor and employees who do the processing of obligations under GDPR and compliance, manages breach procedures, training and expertise in national/European data protection laws. Should be on the website, private notices and data protection policy.

GENERAL DATA PROTECTION REGULATION

INFORMATION COMMISSIONER OFFICE (ICO)

Responsible for safeguarding and enforcing DPA obligations. ICO can issue fines, prosecute, set compensations and other sanctions.

BREACHES

Happen as human error (unless planned criminal activity i.e. e-mail to wrong person. Make risk assessment of data lost and plan remedial action. Any records out of council meetings must be secure, locked away – never left in a car etc. Computers must be encrypted and password protected and never left on. Must not store data on cloud. E-mail is not secure at all and must be password protected or be pdf documents. Personal emails should not be used for business use.

TO DO

Data Mapping – a record of data and how it is stored and used and retained

Reason for processing data – look at consent and what is held.

Policy review – check policies re sharing of information to 3rd parties. (add a line maybe re GDPR)