Coventry Local Safeguarding Children Board

One Minute Guide

GDPR

Number 8, May 2019

GDPR stands for General Data Protection Regulation, and it's a new privacy law which came into effect on 25th May 2018. The aim of the law is to increase the privacy of personal and sensitive information to keep everyone safe, increase transparency and give everyone better control over how their data is collected, shared and used. It's important to take this seriously because there could be penalties if the rules are breached!

There are 6 main responsibilities for everyone:

1	• Personal data should be processed fairly, lawfully and in a transparent manner.
2	• Data should be obtained for specified and lawful purposes and not further processed in a manner that is incompatible with those purposes.
3	• The data should be adequate, relevant and not excessive.
4	• The data should be accurate and where necessary kept up to date.
5	• Data should not be kept for longer than necessary.
6	• Data should be kept secure

ALL staff have a responsibility to comply with the principles

Managers are responsible for the data being collected and how it's used

Each organisation as the data controller are legally responsible for the data being collected and how it's used

Staff should not share data out of line with their organisation's policy, nor for their personal use or gain.

GDPR is **NOT** a barrier to information sharing and should never stand in the way of the need to promote the welfare and safety of children, young people and adults with care and support needs.

If you are ever unsure about sharing information then don't hesitate – check with your manager or use the ICO information link at the bottom of this page.

<u>Personal data</u>

- Relates to an identifiable person
- Is processed electronically or kept in a filing system
- Kept on an accessible record

In the event of a data breach the Information Commissioner's Office must be informed within 72 hours if the breach is identified as causing risk/harm to the data subject

The ICO define a breach as - "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service".

Anything else?

People don't need to be named to be identifiable - the data could relate to a staff number or payroll number!

Check with your Information Governance Lead/Data Protection Officer

Anyone (including staff members) can make a Subject Access Request and organisations must respond to these within a month.

Remember:

- ***GDPR applies to anyone who handles personal data!***
- ***This includes information in notebooks and on Post It notes!***
- ***A clear desk and locking computer screens aids compliance!***

For further Information

Visit the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/