Solihull
METROPOLITAN
BOROUGH COUNCIL

Scope of this Guidance

The following information is for general guidance only. The UK General Data Protection Regulations will define you as a ‘controller’ for the personal information you collect and process. Therefore, you are responsible for its use and must safeguard it.

For this reason, you are strongly advised to seek your own independent advice about your responsibilities and may find it helpful to visit the Information Commissioner’s Office (ICO) website at https://ico.org.uk for further information.

The ICO is the UK regulator for the above legislation and has powers to prosecute and fine any controllers (including individuals) who breach any Data Protection principles. It also offers free advice about your responsibilities.

Your Responsibility to Safeguard Personal Information

The UK General Data Protection Regulations (UK GDPR) and Data Protection Act 2018 (DPA 2018) requires you to take reasonable steps protect the personal information you will hold about children and others. The measures must ensure a level of security appropriate to:

(a) the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage, and

(b) the nature of the information to be protected.

Children’s Personal Information

The UK GDPR provides extra special consideration for children’s personal information. It requires that children need particular protection when you are collecting and processing their personal information because they may be less aware of the risks involved.

If you process children’s personal information then you need to think about protecting it from the outset, and design your systems and processes with this in mind.

The Principles of Data Protection at a glance

1. Lawfulness, fairness and transparency

When you collect personal information, unless it is already apparent you must provide certain information to them such as explaining how you will use the information, whom you may pass it to and why. In this way people can make a fully informed decision whether they want to provide personal information to you.

This is often achieved by including a statement on forms and is referred to as a Privacy Notice. This is known as 'fairness' and should be central to all your processing of children's personal information.

2. Purpose limitation

As described in the first principle, you must be clear about what your purposes for processing the information are from the start. You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent or you have a clear obligation or function set out in law.

3. Data minimisation

Never collect or use more personal information than is needed. Never collect information just in case it might be useful one day.

4. Accuracy

Personal information must be accurate. The measures taken to ensure its accuracy must be proportionate to the harm that could be caused by processing inaccurate information.

5. Storage limitation

Personal information must not be kept any longer than necessary. Once the original purpose for which it was collected (as explained to individuals in your Privacy Notice) no longer exists / the project has finished, the information must be securely and permanently destroyed or erased.

6. Integrity and confidentiality (security)

Keeping personal information safe from unauthorised or unlawful processing or accidental loss, destruction or damage is vital. Here are a few examples of how you can help achieve this.

Sharing Information

- Ensure that no personal information is discussed with anyone or shown to anyone unless they have a lawful need to receive it.
- Password protect ICT equipment and do not let family members use equipment that has the personal data you collect stored on it.
- When at home, do not leave personal information lying around as visitors or family members may see it, or even a burglar. You are not expected to have locked storage but at least take the precaution of storing it out of sight and somewhere you consider to be relatively secure.

Using Passwords

- Always protect memory sticks, laptops, netbook PCs etc. with strong passwords or else the password may be guessed or circumnavigated by unauthorised people and then encryption technologies used to protect them become worthless.

Passwords – What to use

- Use a password that you are able to commit to memory; so you don't have to write it down.
- Think of an easily remembered sentence such as My Eldest Son Is 3 Years Older Than My Youngest Son and then using the capitals of each word you have a strong password - MESI3YOTMYS.
- Another common tip for choosing passwords is to think of three random words and put them together, for example, ZebraCoffeeObligation.

Passwords – What not to use

- Don't use your first or last name in any form.
- Don't use your spouse or partner's name; or that of one of your children.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, your home or street name etc.

- Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a hacker.

- Don't use a word contained in the dictionary (English or foreign language), spelling lists, or other lists of words.