IBSL Information for centres on data protection and the GDPR (General Data Protection Regulation)

This information is intended as basic information for centres and to raise awareness of the new GDPR obligations.

This information should be supplemented by centre's researching and understanding their specific obligations. This information does not represent full or complete details about data protection and the GDPR and should not be relied upon in isolation.

IBSL encourages its centres to find out more and to make sure they are ready for GDPR. Compliance with data protection requirements is part of the IBSL's Centre Agreement.

For more information please go to https://ico.org.uk

The Data Protection Act includes obligations to ensure that personal data is handled fairly and is kept secure.

On 25th May 2018 the GDPR takes effect. Under the GDPR the rights that individuals have over the data that organisations collect and process about them is strengthened.

IBSL require:

- Leaner's full name - to register a learner onto a qualification and for issuing certificates
- ULN (unique learner number) to uniquely identify the learner
    - date of birth – an Ofqual requirement
    - information on disabilities - to inform the monitoring of equal opportunities and success rates of certain groups of learners
    - If any reasonable adjustments are required during assessments
    - Gender – Ofqual requirement
    - Ethnicity – Ofqual requirement

Learners have the right to:

- Enquire how iBSL will ensure the security of personal information
- Ask how long the data will be kept before it is deleted
- Have access to what information is stored about them
- Be given the contact details for the Data Protection Officer

Leaners also have the right to:

- Ensure iBSL collect only minimal data about learners, collecting only what is necessary
- provide/decline consent to use learner's data.
- Enquire what any data collected may be used for
- Ask how data collected is stored

Using Devices Such as Smart Phones, Laptops and Tablets

Where centres may use personal electronic devices for their work, the security of personal data that may be held on these mobile devices can be more at risk. From a data protection point of view, the security and management of personal devices and data held or on them must be considered.

This is often known as 'bring your own device to work' or BYOD.

Using web-hosted email systems such as Gmail to send work related emails, which often contain personal data may not be secure. One option is to use secure remote access which is more secure and improves data protection compliance.

RECAP

The obligation is on the centre to tell people how you use their personal data. Centres can discharge this duty by providing a privacy notice on their website or in any welcome or registration pack given to learners.

Privacy notices need to explain in layman's terms how you use the personal information that you hold. It is important to make the privacy notice available to anyone who requests information about themselves including employees and members of the public.

For more information please go to https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/