Data Protection Policy / UK GDPR

The Data Protection Act 2018 (now amended to the UK GDPR which came into force on January 1st 2021 under the EU Withdrawal agreement) requires that anyone processing personal data must comply with the eight enforceable principles of good practice. Bristol Child Contact Centre will comply with these requirements by ensuring that:

1. BCCC has reviewed the way in which we hold personal data, where it came from and who it is shared with.

2. BCCC has identified our lawful basis for processing and documented them.

3. BCCC has reviewed how we ask for and record consent.

   NB. The GDPR sets a high standard for consent but remember you don't always need consent. You should also assess whether another lawful basis is more appropriate. Consent to process children's personal data for online services is also required. If your business offers online services directly to children, you communicate privacy information in a way that a child will understand. You must provide children with the same fair processing information as you give adults. It will be good practice to also explain the risks involved in the processing and the safeguards you have put in place.

4. Registered with the Information Commissioners Office

5. To fulfil the obligations to data subjects' right to be informed, everyone will receive a copy of the privacy notice. Bristol Child Contact Centre has a process to recognise and respond to individuals' requests to access their personal data.

   Individuals have the right to obtain:
   - confirmation that their data is being processed;
   - access to their personal data; and
   - other supplementary information – this largely corresponds to the information provided in the privacy notice.

Bristol Child Contact Centre also has
- processes to ensure that the personal data you hold remains accurate and up to data,
- a process to securely dispose of personal data that is no longer required or where an individual has asked you to erase it
- procedures to respond to an individual's request to restrict the processing of their personal data.
- processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability.
- procedures to handle an individual's objection to the processing of their personal data.
- processes to identify, report, manage and resolve any personal data breaches.

These are all included in the Privacy Policy.
Adopted February 2021

Reviewed and adopted March 2022

What is the UK GDPR?

The UK GDPR is the UK General Data Protection Regulation [link to legislation.gov.uk]. It is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context,

You may need to comply with both the UK GDPR and the EU GDPR if you operate in Europe, offer goods or services to individuals in Europe, or monitor the behaviour of individuals in Europe. The EU GDPR is regulated separately by European supervisory authorities, and you may need to seek your own legal advice on your EU obligations.

If you hold any overseas data collected before 01 January 2021 (referred to as 'legacy data'), this will be subject to the EU GDPR as it stood on 31 December 2020 (known as 'frozen GDPR'). In the short term, there is unlikely to be any significant change between the frozen GDPR and the UK GDPR.