Kingston Child Contact Centre

Data Protection Policy, with reference to the Secure Storage, Handling, Use, Retention & Disposal of Sensitive Data and Disclosure information

As an organisation holding sensitive data and using the Disclosure Barring service (DBS) to help assess suitability of applicants for positions of trust, Kingston Child Contact Centre (KCCC) complies fully with the Data Protection Act 1998 and the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of sensitive data and disclosure information.

Access is strictly controlled and limited to those who are entitled to see it as part of their duties.

The Data Protection Act 1998 is concerned with the protection of human rights in relation to personal data. The aim of the Act is to ensure that personal data is used fairly and lawfully and that where necessary the privacy of individuals is respected.

Data protection responsibility

Overall responsibility for ensuring that KCCC complies with its data protection obligations rests with The Kingston Child Contact Centre Administrator.

Personal data is data relating to an individual. For KCCC this means, employers, volunteers, members of the Management Committee and families and may be held in manual or computer records.

Sensitive data means data consisting of information relating to an individual's Sensitive information (likely to be included in sickness records and DBS Disclosures), relating to the Equalities Act (2010) 'protected characteristics' as follows:

- Age
- Disability
- Gender reassignment

Marriage and civil partnership

Pregnancy and maternity

Race

Religion or belief

Sex

Sexual orientation

Also including civil or criminal offenses information.

Any Individual is entitled to know what data KCCC holds about them and what it is used for. An individual has the right to have any inaccuracies in data corrected or erased. There is an exemption which allows for non-disclosure of sensitive data if it is held for the purpose of preventing the occurrence of crime due to violence.

Secure Storage and Handling

KCCC abides by eight principles put in place by the Data Protection Act 1998 to make sure that information is handled properly:

- 1 Data is obtained and processed fairly and lawfully.

- 2 Data is held only for specified lawful registered purposes

- 3 Data is adequate, relevant and not excessive.

- 4 Data is accurate and kept up to date.

- 5 Data is not be kept longer than is necessary. (For details – see Appendix 1) (For disposal details – see Appendix 2)

- 6 Data is processed in accordance with the rights of data subjects under this Act.

- 7 Data is kept secure. (For details– see Appendix 3)

- 8 Data will not be transferred outside the European Economic Area unless with the consent of the individual or where the country has adequate systems in place to protect personal data.

Appendix 1 - How long are records kept for?

Records are kept for as long as is deemed necessary, and with reference to the following:

- 1 Financial records need to be held for **6 years**.

- 2 Accident books and paperwork relating to safeguarding or child protection issues about a specific child will be kept indefinitely as children can request this information up to the **age of 21 years.**

- 3 General NACCC guidelines are that information relating to families, staff and volunteers not used for **three years** should be treated as confidential waste and disposed of as such.

Appendix 2 - Disposal

- 1 When personal data needs to be deleted or destroyed, adequate measures are taken to ensure personal data is properly and securely disposed of. This includes the physical destruction of manual files, and the deletion of computer files and back-up files. Particular care is taken over the destruction of manual sensitive data including shredding or disposing via a specialist contractor.

- 2 Computer disposal: All PCs and data storage devices are disposed of

following good data practice. “Boot and nuke” is used to wipe all drives before they are physically destroyed.

Appendix 3 - Secure

• 1 Manual records are kept secure in locked cabinets.

• 2 Individual computers are password protected, with each user having a unique username and password; users are advised to follow safe password practices.

• 3 Sensitive data is identified, so that proper safeguards can be put in place.

• 4 Sensitive documents can also be password protected

• 5 E-mail is not a secure medium for sending confidential information. We request that referrers email completed referral forms are sent as password protected documents or a secure system is used.

• 6 USB Drives. Only password protected drives are used to transfer data to another authorized user. USB drives are routinely wiped after transmission of data.

• 7 Group emails. Group emails within KCCC may be sent with additional recipients displayed. For Emails to addresses outside of KCCC multiple recipients are Bcc'd ('blind carbon copied) to avoid sharing of email addresses (principle 3 of data protection).

• All electronic equipment is purchased, set up and monitored by the KCCC Administrator. Only whitelisted websites are to be accessed in relation to

KCCC work. If a member of the Centre has reason to believe that security or data has been breached, they are to contact the Administrator immediately and not access any files or data pertinent to the Centre until the Administrator has responded.

This policy will be reviewed annually.

AUGUST 2024