DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

TO: Birmingham Children's Trust Community Interest Company

OF: 1 Avenue Road
Aston
Birmingham
B6 4DU

1.1 The Information Commissioner (the Commissioner) issues a reprimand to Birmingham Children's Trust Community Interest Company (BCTCIC) in accordance with Article 58(2)(b) of the UK General Data Protection Regulation (UK GDPR) in respect of certain infringements of the UK GDPR.

1.2 BCTCIC is owned by Birmingham City Council however it works independently of the council in delivering its services. BCTCIC is registered with the ICO as a separate data controller to Birmingham City Council.

1.3 On 10 November 2022 a personal data breach occurred. The breach involved the inappropriate inclusion of some information about another person in a Child Protection Plan (CP plan) by BCTCIC sent to a family.

1.4 The CP plan included personal data relating to children and criminal offence data. This information about the other person was inappropriately accessed when the CP plan was received and read by the recipient. ICO guidance states that if you are collecting and processing children's data it requires particular protection. ICO guidance states that processing criminal offence data carries more risk than other personal data.

1.5 The department that inappropriately disclosed the personal data was BCTCIC's Child Protection and Review (CP&R) department. The CP&R department of BCTCIC aims to offer support to families in the Birmingham area to make a positive difference to their lives. The employees responsible for delivering these services mainly consist of trained social workers.

1.6 BCTCIC's CP&R department regularly processes both personal data relating to children and criminal offence data.

1.7 When the incident occurred BCTCIC was aiming to deliver its services between two neighbouring families, family A and family B. Child X was part of family B. The mother of family A had raised concerns with BCTCIC, regarding the interactions of her child and child X. The data subjects in this matter therefore are all service users.

1.8 The ICO has established that a child protection meeting [redacted] is responsible for creating a CP plan. The process of formulating a CP plan, would take place following an Initial Child Protection Conference (ICPC) meeting. The recorded notes from the ICPC meeting would usually provide the [redacted] with the necessary information to create the CP plan.

1.9 During this process the [redacted] would ordinarily have access to a danger and harms statement. This is because the danger and harms would be part of the meeting agenda during the ICPC. However, on this occasion the danger and harms to family A did not form part of this meeting.

1.10 The [redacted], upon identifying that they could not construct a danger and harms statement from these notes alone, took the initiative to retrospectively access the minutes of a separate strategy meeting between BCTCIC and West Midlands Police, which contained a summary of concerns raised by family A. The [redacted] then copied over the full statement into the danger and harms section of the CP plan.

1.11 Upon completion of the CP plan, the [redacted] then approved the plan for disclosure to family A. As a consequence, the CP plan contained criminal offence data and personal data in error, including identifying information and criminal allegations against child X, that West Midlands Police was investigating that was not appropriate to be disclosed to family A.

Severity of Breach

1.12 The Commissioner has established that the data disclosed included both sensitive criminal data (serious criminal offence allegations made against child X) and personal identifiers of an individual under the age of 18 (child X).

1.13 BCTCIC has not identified any actual harms, however, BCTCIC has acknowledged an expectation of harm in the form of distress to the data subject and family. Additionally, the ICO has identified the following potential consequences:

- Risk of vigilantism, potential physical harm/attacks at home.
- Psychological harms negligently, knowingly, or purposefully paving the way for emotional distress or disturbance (embarrassment, anxiety, fear) to occur.
- Detriment to mental health.
- Loss of sense or control of identity.
- Distressed relationships.
- Loss of confidence.
- Discrimination.

1.14 The Commissioner also considers that despite the personal data itself being retrieved from family A, the personal data in the CP plan was accessed by family A. Had BCTCIC had appropriate technical and organisational measures in place, the risks to the data subjects would have been mitigated.

The reprimand

1.15 The Commissioner has decided to issue a reprimand to BCTCIC in respect of the following alleged infringements of the UK GDPR. BCTCIC was invited to make representations. BCTCIC made representations on 27 February 2024.

- Article 5(1)(f) and Articles 32(1)(b,) and 32(2) which state:

Article 5(1)(f)

1.16 "Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality)."

Article 32(1)

1.17 "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the

risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services."

Article 32(2)

1.18 "In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

1.19 The reasons for the Commissioner's findings are set out below.

Article 5(1)(f) and Articles 32(1)(b) and (2)

1.20 BCTCIC had evidenced some procedures that it believed ensured the security of personal data in this case as follows:

- The standards set out by Social Work England.
- The Initial Child Protection Process Map.
- Quality Assurance Checklist Questions.
- Data Protection Policy.

1.21 The ICO has considered that these policies fall short of achieving appropriate technical and organisational measures to ensure the security of the personal data in this case. This is because they lack prominent and sufficient practical guidance regarding what personal data is inappropriate for release. The initial child protection process map, designates responsibility for ensuring personal data is not included that is inappropriate for release, but no practical guidance on how this is to be achieved. Whilst there is a separate quality assurance checklist, this also does not provide any practical guidance on screening for data that needs redacting. This is coupled with BCTCIC not having any form of secondary or independent review, or corporate redaction policy in place. As the ICO would expect the data protection policy only provides a framework for ensuring compliance, not practical guidance. As such this should support

granular policies and not replace them. As a consequence, sensitive criminal data and personal data relating to a child was disclosed inappropriately to a neighbouring family.

1.22 BCTCIC at the time of the breach relied on the professional standards set out by Social Work England. BCTCIC believed that as social workers aim to meet these standards, this provided them with the appropriate level of expertise in data protection. BCTCIC highlighted two sections that it believed were relevant to data protection. The ICO finds that practice standard two may hold some merit, if combined with robust granular procedures. It is considered the additional standards, however, were not designed, specifically, with data protection compliance in mind. As such Social Work England standards are not an appropriate substitute for internal governance on how BCTCIC's social workers process personal data. Had robust policies been in place then the ICO considers that Social Work England's standards would have been appropriate in a supporting role.

Lack of robust policies

1.23 BCTCIC has failed to provide the ICO with clear evidence of any role specific Standard Operating Procedures (SOPs), processes or policies that ensure staff in the CP&R department can interpret how to apply data protection obligations in a practical sense.

1.24 BCTCIC relied too heavily on the standards set by the Social Work England. Given the size and resource of the controller, the Commissioner would expect BCTCIC to have had bespoke SOPs in place, which focus on the practical application of data protection principles.

Training

1.25 BCTCIC at the time of the breach had in place data protection training for all its staff, regardless of contract. The ICO is encouraged that this was carried out on a mandatory basis at the start of employment, and that it is refreshed annually. BCTCIC should continue to administer its training in this way, as this will ensure it continues to utilise best practice.

1.26 Whilst BCTCIC has an appropriate framework for providing training on data protection principles, for the initial training of its staff and for refresher training to take place, the lack of specific standard operating

procedures in place for social workers to follow, reduces the impact of such training. BCTCIC could have provided granular, role-specific training to its social workers. BCTCIC's data protection team could consider how the concepts of data protection apply to their individual teams, adapting the training appropriately. This could allow for its staff to gain a deeper understanding, and application of their data protection obligations within individual roles.

Mitigating factors

1.27 In the course of the investigation the ICO has noted that:

- BCTCIC contacted West Midlands Police, who confirmed that the data breach would not prejudice its investigation.

Remedial steps taken by BCTCIC

1.28 The Commissioner has also considered and welcomes the remedial steps taken by BCTCIC in light of this incident. In particular:

A) A social worker immediately contacted the neighbour that was inappropriately in receipt of this data and recovered the CP plan on the same day as the disclosure.

B) Family B (family of child X) were informed by post that their child's data with regards to the allegations, had been shared with family A. BCTCIC subsequently conducted a risk assessment.

C) BCTCIC replaced the version of the CP plan, which had previously contained child X's personal data with an updated version.

D) BCTCIC advised family A that the information disclosed is confidential and they must not share the information any further. BCTCIC explained the criminal implications to family A if they share child X's personal data, without the authorisation of BCTCIC.

E) BCTCIC conducted a review of the [redacted] other cases. BCTCIC found no other disclosures in the CP plans drafted by this individual.

F) BCTCIC has completely revised the document template in question (CP Plan). It now has an optional "confidential" section where information can be placed and two outputs can then be generated, one with and one without confidential information. It is now far briefer and there should be

no circumstance in which information should need to be copied and pasted from any other place. BCTCIC's most commonly produced documents have also been revised to minimise this risk. The new CP plan went live on 16 November 2023.

G) Other documents added to BCTCIC's case management system, now require the [redacted] to answer questions about whether the information contained, needs to be withheld. This went live on 16 November 2023.

H) As part of BCTCIC's Information Assurance Plan, all policies and procedures undertaken are undergoing a review.

Decision to issue a reprimand

1.29 Taking into account all the circumstances of this case including the mitigating factors, the Commissioner has decided to issue a reprimand to BCTCIC in relation to the infringements of Articles 5(1)(f), 32(1)(b) and 32(2) of the UK GDPR as set out above.

Further Action Recommended

1.30 The Commissioner has set out below certain recommendations which may assist BCTCIC in rectifying the infringements outlined in this reprimand and ensuring BCTCIC's future compliance with the UK GDPR. Please note that these recommendations do not form part of the reprimand and are not legally binding directions. As such, any decision by BCTCIC to follow these recommendations is voluntary and a commercial decision for BCTCIC. For the avoidance of doubt, BCTCIC is of course required to comply with its obligations under the law.

1.31 If in the future the ICO has grounds to suspect that BCTCIC is not complying with data protection law, any failure by BCTCIC to rectify the infringements set out in this reprimand (which could be done by following the Commissioner's recommendations or taking alternative appropriate steps) may be taken into account as an aggravating factor in deciding whether to take enforcement action – see page 11 of the Regulatory Action Policy Regulatory Action Policy (ico.org.uk) and Article 83(2)(i) of the UK GDPR.

1.32 The Commissioner recommends that BCTCIC should consider taking certain steps to improve its compliance with UK GDPR. With particular reference to Articles 5(1)(f), 32(1)(b) and 32(2) of the UK GDPR, the following steps are recommended:

1.33) BCTCIC should implement a more granular approach to data protection and create a SOP with regards to producing social care documents. The Commissioner recommends the SOP should include a process for any social care product to be independently checked by someone other than the author for personal data, prior to disclosure.

1.34) BCTCIC should create and implement a corporate redaction policy, which ensures staff have the knowledge and tools, to redact the product should it become necessary.

1.35) BCTCIC could also consider what other processes in its departments lead to the disclosure of personal data to service users. Once identified it should consider:

A) Implementing or reviewing appropriate policies and SOPs, at a granular level to mitigate any data protection risks identified. This will ensure each department is equipped to comply with BCTCIC's overarching data protection policy.
B) BCTCIC on completion of such policies and SOPs, should consider training for its staff to ensure these policies and SOPs are understood and implemented by its staff.
C) BCTCIC could engage in dip sampling of work within the first six months, to satisfy itself that the policies and SOPs introduced are effective.

1.36 The ICO invites you to provide feedback on these recommendations, six months from the date of issue. As stated in section 1.30 these recommendations do not form part of the reprimand, therefore, the request for feedback is not legally binding. As such, any decision for BCTCIC to provide feedback is voluntary and a commercial decision for BCTCIC.