DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

TO: Charnwood Borough Council

OF: Southfields Road, Loughborough, LE11 2TU

1.1 The Information Commissioner (the Commissioner) issues a reprimand to Charnwood Borough Council (the Council) in accordance with Article 58(2)(b) of the UK General Data Protection Regulation in respect of certain infringements of the UK GDPR.

The reprimand

1.2 The Commissioner has decided to issue a reprimand to the Council in respect of the following infringements of the UK GDPR:

- Article 5 (1)(f) of the UK GDPR which states that 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)."

The lack of a clear written process for address changes for staff to follow, and the fact that an alert was not put on the file which would have indicated the necessity to be extra vigilant when completing correspondence duties, is evidence that the Council had not done all that may be expected of an organisation that routinely deals with vulnerable service users.

In conclusion, the Council failed to ensure the integrity and confidentiality of the personal data it held for the data subject. Therefore, the Council has allegedly infringed Article 5 (1)(f) of the UK GDPR.

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

The Council is a public authority that routinely deals with members of the public, many of whom will be vulnerable. It would, therefore, be expected that the Council is particularly vigilant when dealing with correspondence that relates to vulnerable service users.

The incident occurred when the Council disclosed the new address of the data subject to her ex-partner. The Council was already aware of

allegations of domestic abuse made against the ex-partner by the data subject when she called to inform the Council of a move to a new address.

A member of staff added the data subject's new address to the notes on the system rather than updating the address field, and there was no evidence that the data subject was informed that she would have to update her [redacted] application herself by logging into it online. As such, the data subject believed her new address details to have been successfully updated.

As this was not the case, the Council sent a letter to her previous address that she shared with her ex-partner, advising of the need to update her [redacted] address. This letter contained her new address and was subsequently confirmed to have been opened and read by her ex-partner.

Due to the previous allegations of domestic abuse, the disclosure of her new address has caused significant distress to the data subject and has the potential to result in harm to the data subject.

In this case, the incident occurred as the process for changing her address was not made clear to the data subject, and through the use of her old address for correspondence, when the member of staff failed to manually transfer the correct address. The system did not have a relevant alert function in place to indicate the necessity for staff to be extra vigilant when dealing with vulnerable service users.

Furthermore, there was an absence of a written and well communicated process for dealing with correspondence in these circumstances for staff to use. In addition, the Council had not ensured that all members of staff, involved in this incident had received data protection training in the twelve months prior to the incident.

It is considered that this incident could have been avoided had there been a robust written process that staff were fully aware of, recent data protection training provided, and an appropriate alert system in place to highlight matters where extra vigilance and checking procedures would be required to ensure the protection of vulnerable service users.

<u>Mitigating factors</u>

1.4 In the course of our investigation we have noted that there are no mitigating factors in this case.

<u>Remedial steps taken by Charnwood Borough Council</u>

1.5 The Commissioner has considered and welcomes the remedial steps taken by the Council in the light of this incident.

Remedial measures taken in the immediate aftermath of the incident were swift and appropriate. The remedial measures that are planned and set out in an Action Plan created by the Council should ensure that a similar incident is much less likely to occur in future.

The examples given of actions noted as completed at the time of this reprimand includes guidance to staff regarding the importance of ensuring data is managed securely and the consequences of breaches, and the incorporation of data protection as a standard item in team meetings and staff one-to-one meetings.

The Council should ensure that all other intended remedial measures are fully implemented. These include a letter creation feature with automatic correspondence address population, the addition of a relevant alert system, and a review of letter templates to ensure these reiterate the requirement for customers to update online applications following a change in address.

When the measures stated by the Council are completed, they should help ensure that a reoccurrence of an incident of this nature is less likely to happen in the future.

Decision to issue a reprimand

1.6 Taking into account all the circumstances of this case, including the mitigating factors and remedial steps, the Commissioner has decided to issue a reprimand to the Council in relation to the alleged infringements of Article 5 (1)(f) of the UK GDPR set out above.

Further Action Recommended

1.7 The Commissioner recommends that the Council should take certain steps to ensure its compliance with UK GDPR.

1. In order to ensure compliance with Article 5 (1)(f) the Council should ensure that all remedial measures stated in its response to ICO enquiries and in the Action Plan are fully implemented as soon as possible.

2. In particular, and in order to support compliance with Article 5 (1)(f), the Council should provide regular refresher training for staff to ensure staff knowledge of the need to be vigilant when processing the personal data of vulnerable service users.

3. In order to ensure compliance with Article 5 (1)(f), the Council should ensure that all staff who may deal with vulnerable service users are provided with robust guidance and training on the correct handling of personal data.