Uncommon

UNCOMMON DATA PROTECTION POLICY

This policy provides a framework for Uncommon's commitment to safeguarding personal data in line with the Data Protection Act 2018 and the UK GDPR. It outlines the principles and responsibilities for handling personal data, ensuring all staff adhere to legal standards for security, privacy, and transparency when processing, storing, and managing sensitive information.

Aim

The Company is committed to complying with its data protection obligations under the Data Protection Act 2018 (the DPA 2018), the UK General Data Protection Regulation 2016/679 (the UK GDPR) and any other applicable UK legislation (together, Data Protection Law).

Purpose

This policy provides a framework for appropriate use of personal data (ie any information which relates to an identifiable individual such as his name or address). For information on how the Company deals with staff members' personal data, please see the staff privacy notice at.

Scope

All staff members (including employees, casual workers, officers and agency workers) must comply with this policy. Any breach of this policy will be taken extremely seriously and, in the case of employees, may lead to disciplinary action up to and including dismissal.

1. The Company's Data Protection Officer is responsible for this policy. If any staff member has any concerns regarding this policy, they should raise these with the Data Protection Officer.
2. The Company will provide training to all staff about data protection on induction and as required thereafter. Staff with responsibility for personal data or whose work involves dealing with personal data on a regular basis will be required to complete additional training. Managers must ensure that they and their staff have completed any required data protection training courses.

Compliance

To comply with data protection law, all staff must act in accordance with the following principles when handling personal data:

a) all personal data must be processed lawfully, fairly and in a transparent way; b) personal data must be collected for specified, explicit and legitimate purposes, and any further processing must be compatible with the original purposes for which the data was collected; c) all personal

data must be adequate, relevant and limited to what is necessary to achieve the purpose for which it is processed; d) all personal data must be accurate and kept up to date where necessary, and all reasonable steps must be taken to correct or erase inaccurate data promptly; e) personal data must not be kept in a form which identifies individuals for any longer than is necessary for the purposes of processing; and f) personal data must be processed securely and in a way that protects against unauthorized or unlawful processing, accidental loss, destruction or damage. Processing personal data includes collecting, using, accessing, organising, disclosing, holding or destroying personal data.

Staff with access to and responsibility for others' personal data:

g) must adhere to the data protection principles listed above; h) must keep personal data secure at all times and comply with the Company's IT, Communications and Social media policy, including the provisions for data security; i) must not access personal data without proper authorisation; j) must not use personal data for unauthorised purposes; k) must exercise proper caution before sharing personal data both within and outside the Company, including by email or via the internet l) must not send others' personal data to their own personal email account or store it on any personal devices; m) must attend and complete any required data protection training; n) must ensure that personal data is not kept for longer than the retention periods specified in the Company's privacy notices; o) must destroy personal data permanently and securely where it is to be deleted p) must report any loss of personal data or personal data breach to the Data Protection Officer as soon as possible; and must inform the Data Protection Officer if they acquire any personal data in error.

Sensitive personal data

From time to time, the Company may process sensitive personal data about an individual. Sensitive personal data is data that is particularly sensitive in terms of the impact it could have on the rights and freedoms of individuals, including personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric and health data, or data concerning a person's sex life or sexual orientation. Such data should typically only be processed with the explicit consent of the individual concerned unless a legal exemption applies. Staff who propose to process any sensitive personal data must notify the Data Protection Officer in order to assess on what basis the data may be processed and to determine whether a DPIA should be carried out. Processing of sensitive personal data must be carried out in accordance with the requirements of this policy at all times.

Data subject requests

Data subjects have various rights in respect of any personal data the Company controls the storage or use of. These include: a) a general right to request a copy of any personal data the Company holds about them, by submitting a Subject Access Request (SAR) to the Company; b) a right to request to transfer or port their personal data (eg to another company); c) a right to request that any inaccurate data held about them is corrected; d) a right to request that any personal data held about them is deleted; and e) the right to withdraw their consent to the

Company's use of their personal data. The Company is under strict legal obligations in relation to some types of requests, therefore any staff member who receives a data subject request (eg from one of the Company's clients, customers, staff, contractors or other relevant person), should immediately pass it to the Data Protection Officer.

Personal data breaches

Staff must immediately report any actual or suspected personal data breaches to the Data Protection Officer so that they can be investigated promptly. The Company is required to notify the Information Commissioner about any sufficiently serious data breaches within 72 hours of discovery, so it is vital that all staff are vigilant and quick to report any suspected breach.

Data protection impact assessments (DPIA)

Where a proposed data processing activity would result in a high risk to the rights and freedoms of individuals, the Company must carry out a DPIA. For example, a DPIA may be required if the Company intends to share personal data with another business, introduces a new IT system or wishes to use personal data on file for a new process. Staff should seek advice from the Data Protection Officer as to whether a DPIA is required in any particular circumstances.