Data Protection Policy

1 Introduction

1.1 Background

The Joint Council for Cosmetic Practitioners The Joint Council for Cosmetic Practitioners (JCCP) Charity is a PSA Approved and recognised self-regulator of the non-surgical aesthetic industry in the UK and the point of access for the public seeking information about this area of practice and where appropriate for raising concerns about practitioners. The JCCP places public protection and patient safety as the focus of its activities.

The JCCP needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include but are not limited to patients, employees (present, past and prospective), suppliers and other business contacts. The information includes name, address, email address, data of birth, private and confidential information, and special categories of personal information. In addition, the JCCP may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or other digital media, on hardcopy, paper or images) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 2018 (the Act).

The lawful and proper treatment of personal information by the JCCP is extremely important to the success of our business and in order to maintain the confidence of our service users and employees. The JCCP must ensure that it processes personal information lawfully and correctly. This policy together with the JCCP Privacy Notice provides information about how we collect and process personal data and the purposes for which we do this.

1.2 Data Protection Principles

The JCCP respects your privacy and is committed to protecting your personal data. We fully support and must be able to demonstrate compliance with the six principles

of the Act which are summarised below:

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Personal data processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

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.

1.3 Information covered by the Act

The Act's definition of "personal data" covers any data that can be used to identify a living individual. Anonymised or aggregated data is not regulated by the Act, providing the anonymisation or aggregation has not been done in a reversible way. Individuals can be identified by various means including their name and address, telephone number or Email address.

The Act defines special categories of personal data (previously referred to as sensitive personal information) as information related to:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sexual history and/or sexual orientation
- Criminal data

2 Scope

We limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

3 Roles and Responsibilities

3.1 The JCCP will: -

- Ensure that an appropriate framework is in place encompassing relevant roles within the organisation that have responsibility for data protection, including the Data Protection Officer
- Provide training for all staff who handle personal information and ensure access to further guidance and support
- Provide clear lines of report and supervision for compliance with data protection
- Carry out regular checks to monitor and assess new processing of personal data and to ensure the JCCP notification to the Information Commissioner is updated to take account of any changes in processing of personal data
- Develop and maintain Data Protection procedures to include roles and responsibilities, notification, subject access, training and compliance testing
- Maintain a record of processing activities
- Ensure the organisation complies with its transparency and fair processing obligations in relation to data subjects' personal data

3.2 The Data Protection Officer

Our Data Protection Officer is Kirsty Benn-Harris who is responsible for overseeing questions in relation to this policy. If you have any questions about this policy, please email admin@jccp.org.uk

3.3 Employee Responsibilities

All employees will, through appropriate training and responsible management:

- Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information.
- Understand fully the purposes for which the JCCP uses personal information.
- Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by the JCCP to meet its service needs or legal requirements.
- Ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required.

- On receipt of a request by or on behalf of an individual for information held about them, or any other data subject's rights in relation to their personal data, staff will immediately notify their line manager and the customer contact centre and abide by the Procedure for managing personal data requests.

- Not send any personal information outside of the United Kingdom without the authority of the Data Protection Officer.
- Understand that breaches of this Policy may result in disciplinary action, up to and including dismissal.

4 Distribution and Implementation

4.1 Distribution Plan

This document will be made available to all staff via their induction and will be available via the JCCP website.

5 Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Data Protection Officer.

JCCP

September 2021