TATTOOS AND PIERCINGS

DATA PROTECTION & DATA SECURITY POLICY

Statement and purpose of policy

A. Gemma Gallagher (the Employer) is committed to ensuring that all personal data handled by us will be processed according to legally compliance standards of data protection and data security.

B. We confirm for the purposes of the data protection laws, that Gemma Gallagher is a data controller of the personal data in connection with your business with us. This means that we determine the purpose of which, and the manner in which, your personal data is processed.

C. The purpose of this policy is to help us achieve our data protection and data security aims by:

1). Notify our customers of the types of personal information that we may hold about them, our suppliers and other third parties and what we do with that information;

2). setting out the rules on data protection and the legal conditions that must be satisfied when we collect, receive, handle, process, transfer, and store personal data and ensuring staff understand our rules and the legal standards; and

3). clarifying the responsibilities and duties of the Employer in respect of data protection and data security.

D. This is a statement of policy only, and does not form part of your consumer contract with us. We may amend this policy at any time in our absolute discretion.

E. For the purposes of this policy:

1. Data protection laws means all applicable laws relating to the processing of personal data, including, for the period during which it is in force, the UK General Data Protection Regulation.

2. Date subject means the individual to whom then personal data relates.

3. **Personal data** means any information that relates to an individual who can be identified from that information.

4. **Processing** means any use that is made of data, including collecting, storing, amending disclosing or destroying it.

5. **Special categories of personal data** means information about an individual's racial or ethical origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

Data protection principles

1. Staff whose work involves using personal data relating to customer must comply with this Policy and with the following data protection principles required that personal information is:

a. **Processed lawfully, fairly and in a transparent manner:** We must always have a lawful basis to process personal data, as set out in the data protection laws. Personal data may be processed as necessary to perform a contract with the data subject to comply with a legal obligation which the data controller is the subject of, or for the legitimate interest of the data controller or the party to whom the data is disclosed. The data subject must be told who controls the information (us), the purpose(s) for which we are processing the information and to whom it may be disclosed.

b. **Collected only for specified, explicit and legitimate purposes.** Personal data must not be collected for one purpose and then used for another. If we want to change the way we use personal data, we must first tell the data subject.

c. **Processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing**. We will only collect personal data to the extent required for the specific purpose notified to the data subject.

d. **The employer takes all responsible steps to ensure that information that is inaccurate is rectified or deleted without delay.** Checks to personal data will be made when collected and regular checks must be made afterwards. We will make reasonable efforts to rectify or erase inaccurate information.

e. **Kept only for the period necessary for processing**. Information will not be kept longer than it is needed and we will take all reasonable steps to delete information when we no longer need it. For guidance on how long particular information should be kept, contact the Data Protection Officer.

f. Secure and appropriate measures are adopted by the employer to ensure as such.

Who is responsible for data protection and data security?

2. Maintaining appropriate standards of data protection and data security is a collective task shared between us and you, this policy and the rules contained in it apply to the employer irrespective of seniority, tenure and working hours, including all employees directors and officers consultants and contractors, trainees and fixed team staff.

3. Questions about this policy, or request for further information should be directed to the data protection officer.

4. All staff have a Personal responsibility to ensure clients with this Policy, to handle all personal data consistently with the principals set out here and to ensure that measures are taken to protect the data security. Managers have special responsibility for leading by example and monitoring and enforcing compliance. The Data Protection Officer must be notified if this policy has not been followed, or if it is suspected this policy has been followed, as soon as reasonably practical.

5. Any breach of this policy will be taking seriously and may result in disciplinary action up to and including dismissal. Significant or deliberate breaches, such as accessing customer personal data without authorisation or the legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

What Personal Dating and Activities are Covered by This Policy?

6. This policy covers personal data:

a. Which relates to a natural living individual who can be identified either from that information in isolation or by reading it together with other information we possess;

b. Is electronically or on paper in a filing system;

c. In the form of statements of opinion as well as facts;

d. Which relates to staff (present, past or future) or any order individual whose personal data we handle or control;

e. Which we obtain, is provided to us, which we hold or store, organise, disclose, or transfer, amend, retrieve, use, handle, process, transport, or destroy;

7. This personal data is subject to the legal safeguards set out in the data protection laws.

What Personal Data Do We Process About Staff?

8. We collect personal data about you which;

a. you provide or we gather before or during your engagement with us;

b. is provided by you either through the website when booking or on the business premises with a consent form.

9. The types of personal data that we may collect, store and use about you include records relating to your:

a. full legal name, home address, contact details and medical history.

Sensitive personal data

We may from time to time need to process sensitive personal information (sometimes referred to a 'special categories or personal data')

11. We will only process sensitive personal information if we have a lawful basis for doing so, e.g. it is necessary for the performance of the appointment contract; and
b. one of the following special conditions for processing information applies:

i. The data subject has given explicit consent

ii. The processing is necessary for the purpose of exercising the Employer law rights of obligations of the company or the data subject.

iii. The processing is necessary to protect the data subject's vital interests, and their data subject is physically incapable of given consent.

iv. Processing relates to personal data which are manifestly made public by the data subject.

v. The processing is necessary for the establishment exercise or defence or legal claims; or

vi. The processing is necessary for reasons of substantial public interest.

12. Before processing any sensitive personal information, Staff must notify the Data Protection Officer of the proposed processing, in order for the Data Protection Officer to assess whether the processing complies with the criteria noted above.

13. Senses of personal information will not be processed until the assessment above as taken place and the individual has been promptly informed of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

14. Our privacy notice sets out the type of sensitive personal information that we process, what is used for and the lawful basis for the processing.

How We Use Your Personal Date

15. We will tell you the reasons for processing your personal data, how we use such information and the legal basis for processing in our Private Notice.

16. In general, we will use information to carry out our business, to administer your service and engagement and to deal with any problems or concerns you may have, including, but not limited to;

a. Compile of home addresses and contact details

b. To maintain a record of your medical history and any medications that you may be taking

c. Monitor use of emails internet telephone or communications you have with ourselves

d. Disciplinary grievance or legal matters: in connection with any grievance, legal, regulatory, or compliance matters or proceedings that may involve you.

e. Performance reviews: to carry out performance reviews.

Accuracy and Relevance

17. We will:

a. ensure that any personal data process is up to date, accurate, adequate, relevant and not excessive, given the purpose for which it was a collected.

b. not process personal data obtained for one purpose for any of the purpose, unless you agree to this or reasonably expect this.

18. If you consider that any information held about your is inaccurate or out of date, then you should tell the Data Protection Officer. If they agree that the information is inaccurate or out of date, then they will correct it promptly. If they do not agree with the correction, then they will note your comments.

Storage and Retention

19. Personal data and (sensitive personal information) will be kept securely in accordance with our Information Security Policy.

20. The periods for which we hold personal data are contained in our Privacy Notes.

Individual rights

21. You have the following rights in relation to your personal data.

22. Subject access request:

a. You have the right to make a subject access request if you make a subject access request we will tell you.
i. Whether or not your personal data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from you.
ii. To whom your personal data is or maybe disclose.
iii. For how long your personal data is stored or how that period is decided.
iv. Your rights of rectification or erasure of data, or to restrict or object to processing;
v. Your right to write to complain to the Information Commissioner if you think we have failed to comply with your data protection right; and
vi. whether or not we carry out automated decision-making and the logic involved in any such decision making.

b. We will provide you with a copy of the personal data undergoing processing. This will normally be in electronic form if you have made a request electronically unless you agree otherwise.

c. To make a subject access request, contact us at info@gemmagallagher.com

d. We may need to ask for proof of identification before your request can be processed. We will let you know if we need to verify your identity on the documents we require.

e. We will normally respond to your request within 28 days from the date your request is received. In some cases for example where there is a large amount of personal data being processed we may respond within three months of the date your request is received. We will write to you within 28 days of receiving your original request if this is the case.

f. If you're request is manifestly unfounded or excessive we are not obliged to comply with it.

23. Other rights

a. You have a number of other rights and relation to your personal data. You can require us to:

i. rectify inaccurate data;

ii. stop processing or erase data that is no longer necessary for the purpose of processing.

iii. stop processing erase data if your interests override our legitimate grounds for processing the data (where we rely on our legitimate interests at a reason for processing and data);

iv. stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override the employers legitimate grounds for processing the data.

b. To request that we take any of these steps, please send the request to info@gemmagallagher.com

Data Security

24. We will use appropriate technical and organisation or measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss destruction or damage.

25. Maintaining data security means making sure that:

a. only people who are authorised to use the information can access it;

b. Where possible, personal data is pseudonymised or encrypted;

c. Information is accurate and suitable for the papers for which it is processed; and

d. Authorised persons can access information if they need it for authorized purposes.

26. By law, we must use procedures and technology to secure personal information throughout the period that we hold or control it, from obtaining to destroying the information.

27. Personal information must not be transferred to any person to process (e.g while performing services for us or on behalf), unless that Pearson has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.

28. Security procedures include:

a. Any desk, cupboards or filing systems containing confidential information must be kept locked.

b. Computers should be locked with a strong password that change regularly or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.

c. Data stored on CDs or memory sticks must be encrypted or password-protected and locked away securely when they are not being used.

d. The data protection officer must approve of any cloud used to store data.

e. Data should never be saved directly to mobile devices such as laptops tablets or smartphones.

f. All servers containing sensitive personal data must be approved and protected by security software.
g. Servers containing personal data must be kept in a secure location, away from general office space.

h. Data should be regularly backed up in line with the employers backup procedure.

29. Telephone precautions. Particular care must be taken by staff who deal with the telephone enquiries to avoid inappropriate disclosures. In particular:

a. The identity of any telephone caller must be verified before any personal information that's disclosed;

b. If the caller's identity cannot be verified satisfactorily then they should be asked to put their query in writing.

c. Do not allow callers to bully you into disclosing information. In case of any problems or uncertainty contact the Data Protection Officer.

30. Methods of disposal. Copies of personal information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable.

31. Additional measures to ensure data security include:

When you book an appointment through our website you will be asked for your full name, email address and home address along with your telephone number and payment details. The only details we have access to are your contact details and will only use these if in the (very rare) event we have to reschedule your appointment.

Any correspondence done via emails or text will be sent from a password protected business only laptop or our business phone.

When you attend your appointment you are required to fill in a consent form and may be required to provide government issue photo ID, which is a requirement for our local authority. The information we collect includes:
a. Name
b. Home address
c. Email address
d. Telephone number
e. Date of birth
g. Medical history

Where photo ID is required, we will take a copy of this and attach it to your consent form. All documents including appointment diaries that hold client data is kept in a locked filing cabinet which is situated in a locked room, only accessible to the business owner.

Your personal information is not shared with other businesses or organisations. However, the local Council could request the right to access all consent forms in the events of a problem, but this would be very rare.
We only use the above information to confirm your consent and identity.

If you have any questions in relation to the above, you can contact us on the email below.
info@gemmagallagher.com

Data Impact Assessments

32. Where processing would result in a high risk to customer rights and freedoms, the Employer will carry out a data protection Impact Assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data Breaches

33. If we discover that there has been a breach of customer personal data that poses a risk to the rights and freedoms of individuals we will report it to the Information Commissioner within 72 hours of Discovery.

34. We will record all data breachers regardless of their effects in accordance with our breach response policy.

35. If the breach is likely to result in a high risk to your rights and freedoms we will tell effected individuals that there has been a breach and provide them with more information about its likely consequences and the mitigation measures it has taken.

Individual Responsibilities

36. As a customer it is you're responsibility to let the employer of the business now if personal data provided to the employer changes, e.g. if you move house or change your number.

Individuals who have access to personal data on required:
a. To access only personal data that they have authority to access and only full authorised purposes;

b. not to disclose personal data except to individuals (whether inside or outside of the Employer) who have appropriate authorisation;

c. To keep personal data secure (e.g. by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

d. Not to remove personal data or devices containing or that can be used to access personal data, from the Employers premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and

e. not to store personal data on local drives or personal devices that are used for work purposes.

Training

37. Individuals whose roles require regular access to personal data, or who are responsible for implementing this Policy or responding to subject access requests under this Policy will receive additional training to help them understand their duties and how to comply with them.