**esig.png**

**Fleet Recruitment Ltd Data Protection and Security Policy**

**Statement of policy and purpose of policy**

Fleet Recruitment is committed to ensuring that all personal information handled by us in relation to employees, clients and candidates will be processed accordingly to legal compliant standards of data protection and data security.

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

1. Notifying our staff and candidates about the types of personal information we might hold about them and what we do with that information.
2. Ensuring our staff understand our rules and the legal standards for handling personal information relating to our colleagues, clients and candidates.
3. Clarifying the responsibilities and duties of staff in respect of data protection and security.

**Who is responsible for data security?**

4. Maintaining appropriate standards of data protection and data security is a collaborative task between Fleet Recruitment Ltd and our employees. This policy and the rules contained within it apply to all staff and associates, irrespective of seniority or working location.

5. The Managing Director has overall responsibility for ensuring that all personal and candidate information is handled in compliance with the law and is the data protection officer with day to day responsibility.

6. All employees and associates of Fleet Recruitment have personal responsibility to ensure compliance with this policy, to handle all personal information consistently with the principals set out here and to ensure that measures are taken to protect data security. You are all expected to lead by example by monitoring and enforcing compliance.

**What personal information is covered by this policy?**

This policy covers personal information:

1. Which relates to any living individual who can be identified either from the information we hold in isolation or by reading it together with other information we possess.
2. Is stored electronically or on paper based systems
3. in the form of statements of opinion as well as facts
4. which relates to staff, clients or candidates past or present or to any other individual whose personal information we hold or control
5. which we hold, obtain, store, organise, disclose, transfer, amend, retrieve, use, handle, process, transport or destroy.

**What personal information do we process and what we do with it**

9. We collect information about you and candidates which:

a. You provide or we gather during your employment with Fleet Recruitment

b. Is provided by third parties, candidates, referees or any other third party that we do business with.

c. Is in the public domain.

10. The types or person information we may collect, store and use in relation to you, our clients or our candidates relates to:

a. Home address and contact details

b. Recruitment, including qualifications, application forms and CVs

c. National insurance numbers

d. Pay records

e. Sickness absence and medical records

f. information about race, colour, religious beliefs, ethic or national origins

g. Sexual orientation

h. email addresses, contact telephone numbers

i. dates of birth

**Your responsibilities**

1. All candidate CVs are to be stored electronically on our CRM system. Paper copies should be shredded using the shredder provided. When CVs have been printed they are not to be left in any areas where they could be overseen by any other person other than Fleet Recruitment Employees.
2. Emails containing CVs or personal data should be deleted once that information is recorded to the secure CRM.
3. Computers and laptops must be password protected and all windows updates accepted
4. No CVs are to be stored on Laptops or Desktops. They must be uploaded to the company CRM and immediately deleted from Laptops and Desktops.
5. Passwords must be changed every four weeks including, your laptop / desktop access and the CRM system. The password must be constructed of three random works connected with random symbols.
6. You must not send e-mails containing CVs as an attachment using unsecure public wifi such as in internet cafes, etc.
7. Candidates should not be contacted for any other reason than those related to recruitment and supporting them into a new job.
8. All candidate information remains the property of Fleet Recruitment and is highly confidential. You must not pass personal information to any third party without the express permission of the candidate.
9. You must take responsibility to protect sensitive candidate information including all the information detailed in point above.

**You must:**

1. Ensure that all personal data is collected with customers' consent.
2. Not use personal data for any purpose other than that for which consent was given, respecting customers' wishes about the use of their data.
3. Make sure that customers have access to their personal data that we hold and tell them how we use it.
4. Make every possible effort to protect personal data and keep it secure and confidential.
5. Remember that personal data is just that – personal – You must ensure that it is treated with respect.
6. Manage our data supply chain to the same ethical standards we expect from other suppliers.
7. Ensure that ethical best practice in personal data is integral to our procurement process.
8. Ensure that you ask for advice if you are unsure about any aspect of your responsibilities regarding personal data.
9. Not use personal data if there is uncertainty as to whether the Fair Data Principles have been applied.
10. Any breaches must be reported to the managing Director, who in turn will report the matter to the ICO. Employees reporting the breech must record the details on the IT security event log, located in the company cloud based shared drive.

**Failure to abide by these rules will be treated as a serious breach of trust and will lead to disciplinary action that may or may not lead to your dismissal.**