1. Policy Statement

1.1. This policy outlines Pro-Force's procedures in relation to collecting, processing and storing personal and sensitive data.
1.2. Pro-Force takes the security and privacy of personal data seriously. Pro-Force needs to gather and use information about data subjects as part of our business activities and in order to provide services.
1.3. In respect of our obligations under the Data Protection Act 2018 (the Act) and the EU General Data Protection Regulations (GDPR), Pro-Force has a duty to notify all data subjects of the information contained in this policy.
1.4. Pro-Force commits to act within the bounds of the relevant data protection laws within all of the countries that it operates in.

2. Scope of the policy

2.1. This policy is applicable to all Pro-Force branches, sites and locations across the UK, any Company that falls into the Pro-Force Group, and to all staff members including directors, senior managers, managers, officers, employees, volunteers (collectively referred to as staff in this policy) and additionally to work seekers, former employees and individual client contracts.
2.2. Anyone who falls into one of these categories is considered a "data subject" for the purposes of this policy.
2.3. This policy does not form part of the contract of employment for employees, and as such, Pro-Force reserves the right to amend the policy at any time.

3. Responsibility for implementation of the policy

3.1. The Managing Director and the Senior Leadership Team have overall responsibility for the implementation of this policy.
3.2. The compliance department is responsible for monitoring and reviewing the operation of this policy and making recommendations for changes to minimise risk to operations.
3.3. Line managers and supervisors are required to familiarise themselves with, and understand this policy, it's operation, and any related procedures. Compliance will provide training documentation and guidance on the provisions of this policy, as is relevant to their responsibilities.
3.4. Questions related to the use, understanding or direction of this policy should be directed to the Compliance department.
3.5. Pro-Force is registered with the ICO and its registration number is: Z9297919. Pro-Force is a "data controller" for the purposes of processing personal data, and therefore we determine the purpose and means of processing personal data. Pro-Force will only process personal data where it has a legal basis for doing so.
3.6. Pro-Force's Privacy Notice is available via www.pro-force.co.uk. Pro-Force will review the personal data it holds on a regular basis to ensure that it is being lawfully processed, is accurate, relevant and up to date.
3.7. Prior to transferring information to a third party, Pro-Force will establish that it has a legal basis for doing so. It is intended that this policy and associated procedures, notices and documents are compliant with the Act and the GDPR. If any conflict arises between those laws and this policy, Pro-Force intends to comply with the Act and the GDPR.

4. Data Protection Principles

4.1. All personal data must be processed in accordance with our Data Protection Principles. It must:

- Be processed fairly, lawfully and transparently;
- Be collected and processed only for specified, explicit and legitimate purposes;
- Be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- Not be kept for longer than is necessary for the purposes for which it is processed;
- Be processed in accordance with the rights of data subjects;
- Not be transferred to another country without appropriate safeguards being in place; and
- Be processed securely.

4.2. Pro-Force is accountable for these principles and must be able to demonstrate compliance with them.

5. Defining personal data

5.1. "Personal data" means information which relates to a living person who can be identified from that data (a "data subject") on it's own, or when taken together with other information is likely to come into our possession. It does not include anonymised data. This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

5.2. This personal data may be provided to Pro-Force by data subjects, other persons, or could be created by Pro-Force. It could be provided or created during the recruitment process or during the course of work, or after its termination. It could be created by Pro-Force staff members.

5.3. We collect and use the following types of personal data

- Recruitment information such as registration packs and CVs, references, qualifications, memberships of professional bodies and details of any pre-employment assessments
- Contact details and dates of birth
- Emergency contact details / next of kin details
- Gender
- Marital status and family details
- Information about employment contracts or contract for services including start / end dates, role, location, working hours, promotion, salary / pay rates, pension, benefits and holiday entitlement
- Bank details and information relating to tax status such as national insurance numbers
- Identification documents such as passports, ID cards and driving licence, and other documents relating to immigration status / right to work
- Information relating to disciplinary / grievances / complaints and dispute investigations
- Information relating to performance / behaviour whilst at work
- Training records and documents
- Electronic information in relation to use of IT systems and telephone systems
- Images (photographs, video, CCTV)
- Any other category of personal data which Pro-Force will notify data subjects of from time to time

5.4. We might collect and use special categories of personal data in accordance with the law, such as:

- Racial / ethnic origin
- Trade union membership
- Genetic / biometric data
- Health
- Criminal convictions or offences

5.5. We use this information only within designated purposes, for example ethnic origin to determine the right to work in the UK, as expanded on below.

6. Defining processing

6.1. Processing means any operation which is performed on personal data such as:

- Collection, recording, organisation, structuring or storage
- Adaptation or alternation
- Retrieval, consultation or use
- Disclosure by transmission, dissemination or otherwise making available
- Alignment or combination, and
- Restriction, destruction or erasure

6.2. This includes processing personal data which forms part of a filing system or any automated processing.

7. How Pro-Force processes personal data

7.1. We will use your personal data for:

- Compliance with a legal obligation (e.g real time information reporting to HMRC)
- The performance of the contract (e.g processing payroll, monitoring attendance)
- Protecting the legitimate interest of the company or third party (e.g. collecting information during disciplinary, grievance, complaints, or disputes process, or collecting workplace data in order to improve workplace performance). You have the right to challenge our legitimate interests and request that we stop this processing – see the section on data subject access rights for further detail.

7.2. Pro-Force can process personal data for these purposes without specifically informing data subjects or obtaining consent. Pro-Force will not use personal data for an unrelated purpose without informing the data subject and the legal basis that is relied on for processing it.

7.3. If a data subject chooses not to provide Pro-Force with personal data, they must be aware that Pro-Force will be unable to carry out certain parts of the contract between Pro-Force and the data subject. For example, an employee who does not wish to provide bank details may result in Pro-Force not being able to pay them, or stopping Pro-Force being able to comply with legal obligations such as payment of tax to HMRC.

8. Privacy by design and default

8.1. Pro-Force is required to demonstrate that privacy considerations are embedded in all our processes and procedures. Data impact assessments are completed on our processes when updated or changed to ensure compliance with the principles of the GDPR.

8.2. The types of measures that we have implemented include:

- Data minimisation (not keeping data for longer than is necessary)
- Cyber security
- Data protection principles training and procedures

9. Examples of data processing

9.1. Pro-Force has to process personal data in various stations during recruitment, employment or engagement for work, and even after employment or engagement, such as:

- Deciding whether to employ or engage individuals
- Deciding how much to pay individuals and other terms of contract
- Checking individuals have the right to work in the UK
- In order to carry out the contract between individuals and Pro-Force, including where relevant, it's termination
- Training and reviewing performance
- Promotion decisions
- Deciding whether and how to manage performance, absence or conduct
- To carry out disciplinary, grievance or complaints investigations
- Determining whether reasonable adjustments to workplaces or roles because of disabilities
- Monitor diversity and equal opportunities
- Monitor and protect the security of Pro-Force, employees, workers, clients, customers and others
- Monitor and protect the health & safety of employees, workers, clients, customers and others
- To pay staff and provide pension and other benefits in accordance with the contract
- Paying tax and national insurance
- To provide a reference upon request from another employer
- To pay trade union subscriptions, if relevant
- Monitoring compliance with policies and contractual obligations
- To comply with employment law, immigration law, health & safety law, tax law and other laws which affect Pro-Force
- To answer questions from insurers in respect of relevant insurance policies
- running the business and planning for the future
- Preventing and detection of fraud and other criminal offences
- To defend Pro-Force in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure
- For any other reason which we may notify you of from time to time

9.2. Pro-Force may process special categories of personal data in certain situations in accordance with the law. We do not need your consent to do so when we are processing for the following purpose:

- Where it is necessary for carrying out rights and obligations under employment law
- Where the data is public
- Where the processing is necessary for establishment, exercise or defence of legal claims
- Where processing is necessary for the purposes of occupational medicine or for assessment of working capacity

9.3. In particular, we will use information relating to:

- Race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities
- Sickness absence, health and medical conditions to monitor absence, assess fitness for work, pay benefits, comply with legal obligations under employment law including to make reasonable adjustments and to look after health and safety
- Trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members (as is applicable)
- Self disclosure of unspent criminal convictions only in accordance with the Rehabilitation of Offenders Act 1979

9.4. Pro-Force does not make automated decisions about individuals, or use personal data or profiling in relation to staff, except where the automated profiling / decision is:

- Necessary for entering into or performance of a contract between Pro-Force and an individual
- Authorised by law
- Explicit consent is provided

10. Sharing personal data

10.1. Pro-Force may share personal data with group companies, contractors, clients and other agents to carry out obligations under contract for other legitimate interests, such as external audits.

10.2. Pro-Force requires all companies to keep personal data confidential and secure, and to protect it in accordance with the law and relevant policies. They are only permitted to process personal data for the lawful purpose for which it has been shared and in accordance with Pro-Force instructions.

10.3. Circumstances where Pro-Force will share personal data include:

- Sharing with HMRC for tax purposes
- Sharing with clients for providing work finding services
- Sharing with clients and authorised audit bodies for audit purposes

10.4. Pro-Force does not send personal data outside the European Economic area. If this ever changes, individuals will be notified of this and the protections which are in place to ensure the data is secure.

11. Data responsibilities

11.1. Individuals who work for, or on behalf of Pro-Force, has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and related policies.

11.2. The compliance department is responsible for reviewing this policy and updating Pro-Force's data management and data protection procedures. Questions regarding this policy should be directed to the compliance department on 01227 733 880 or enquiries@pro-force.co.uk

11.3. The following details are key rules and good practice that apply to everyone in Pro-Force that processes personal data, and those processing data may be subject to monitoring, inspection and risk assessment to ensure that they are being applied.

- Do not share data outside of Pro-Force.
- Only use data for the purposes it was intended e.g. recruitment, paying workers
- Do not make unnecessary copies of personal data e.g. payslips, work records, hours etc.
- Use strong passwords.
- Do not save personal data or any work information anywhere other than on RDS or Opera.
- Do not save personal data to your own computer or any other devices such as phones.
- Lock computer screens when not at desks.
- Always log out of RDS.
- Lock drawers and filing cabinets.
- Do not leave paper with personal data on lying about.
- Do not take personal data home without the permission of the relevant manager.
- Dispose of data properly – always shred it.
- Any deliberate breach of data protection procedures may result in disciplinary action.
- Do not ignore Data Subject Access requests – pass them onto the compliance department.
- If you think there has been a breach of data, report to the management team. Keep any evidence in relation to this.

12. Dealing with data breaches

12.1. Pro-Force has robust measures in place to minimise and prevent data breaches from taking place. If a breach of personal data occurs, then notes and evidence of the breach must be taken and retained. If the breach is likely to result in a risk to the rights and freedoms of individuals, then the Information Commissioners Office must be notified within 72 hours. If anyone within Pro-Force becomes aware of a data breach, contact the compliance department.

13. Subject access requests

13.1. Data subjects can make a "subject access request" (SAR) to find out what information Pro-Force holds on them. This request must be made in writing. If such a request is received, it must be forwarded to the compliance department who will coordinate a response.

13.2. If an employee or worker would like to make a SAR in relation to their own personal data, this must be made in writing to the compliance department. Pro-Force will respond within 30 days (unless the request is complex or numerous in which case the period can be extended by a further two months).

13.3. There is no fee for making a SAR. However, if the response is manifestly unfounded or excessive, Pro-Force may charge a reasonable administrative fee or refuse to respond to the request.

14. Data Subjects Rights

14.1. All data subjects have the right to:

- Information about what personal data Pro-Force processes, how and what basis as set out in this policy and privacy notices.
- Access to their own personal data by way of a subject access request
- Correct any inaccuracies in their personal data
- Request personal data is erased where Pro-Force is not entitled under the law to process it, or where it is no longer necessary to process it for the purpose it was collected.
- Object to data processing where Pro-Force is relying on a legitimate interest to do so, and the data subject's rights and interests outweigh that of Pro-Force
- Object if personal data is processed for direct marketing purposes
- Receive a copy of personal data and transfer personal data to another data controller
- Not to be subject to automated decision making
- Notified of a data security breach concerning personal data
- Data portability which allows data subjects to access their personal data and reuse it for their own purposes
- Complain to the Information Commissioner directly.

14.2. In most situations Pro-Force will not rely on consent as a lawful ground to process data. If however, this is requested, data subjects will have the right not to consent, or if consent is given, withdraw that consent later. To withdraw consent, individuals should contact the compliance department on 01227 733 880 or via enquiries@pro-force.co.uk

15. Data Retention

15.1. Pro-Force will retain data in line with requirements under law or where it is in our legitimate interest to retain the data.

16. Policy Review

16.1. The compliance department is responsible for reviewing this policy annually, or as is required, to ensure that it meets legal standards and reflects best practice.

Matthew Jarrett

CEO
Pro-Force Limited