WRUK LTD T/A WORKSHOP RECRUITMENT
DATA PROTECTION AND INFORMATION SECURITY POLICY
Effective Date: 08 June 2026
Review Date: Annually
Policy Owner: Directors

1. POLICY STATEMENT

WRUK Ltd ("the Company") is committed to protecting personal data, confidential information and Company information assets.
As a recruitment business, we process information relating to candidates, temporary workers, clients, suppliers and employees. We recognise the importance of handling such information responsibly, securely and lawfully.
The Company is committed to:
• Complying with UK GDPR and the Data Protection Act 2018.
• Protecting the confidentiality, integrity and availability of information.
• Maintaining appropriate information security controls.
• Preventing unauthorised access, disclosure, loss or misuse of information.
• Promoting a culture of security awareness.
Failure to comply with this policy may result in disciplinary action and, in serious cases, dismissal.

2. PURPOSE

The purpose of this policy is to:
• Protect personal data and confidential information.
• Ensure compliance with legal obligations.
• Reduce cyber security risks.
• Establish security responsibilities.
• Provide guidance on handling information securely.
• Support business continuity and operational resilience.

3. SCOPE

This policy applies to:
• Employees.
• Directors.
• Temporary workers provided with access to Company systems.
• Contractors.
• Consultants.
• Agency workers.
• Any third party granted access to Company information.
The policy applies to information held:
• Electronically.
• On paper.
• In cloud-based systems.
• On mobile devices.
• In emails and communications.

4. DEFINITIONS

Workshop Recruitment
Ashville House, 260-262 Havant Road, Drayton,
Portsmouth, Hampshire PO6 1PA England
Tel: 023 9232 4666
Fax: 023 9232 4777
Email: mail@workshoprecruitment.co.uk

Personal Data
Any information relating to an identifiable individual.
Examples include:
• Names.
• Addresses.
• Telephone numbers.
• Email addresses.
• Employment history.
• CVs.
• Payroll information.
• Identification documents.

Special Category Data
Personal information requiring additional protection, including information relating to:
• Health.
• Ethnic origin.
• Religious beliefs.
• Trade union membership.
• Sexual orientation.
• Biometric information.

Confidential Information
Information which is not publicly available and which relates to:
• Candidates.
• Clients.
• Temporary workers.
• Employees.
• Financial information.
• Business plans.
• Commercial arrangements.

Data Breach
A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

5. DATA PROTECTION PRINCIPLES
The Company will ensure personal data is:
• Processed lawfully, fairly and transparently.
• Collected for specified purposes.
• Adequate, relevant and limited to what is necessary.
• Accurate and kept up to date.
• Retained only for as long as necessary.
• Protected against unauthorised access, loss or damage.
• Processed in accordance with individuals' rights.

Workshop Recruitment
Ashville House, 260-262 Havant Road, Drayton,
Portsmouth, Hampshire PO6 1PA England
Tel: 023 9232 4666
Fax: 023 9232 4777
Email: mail@workshoprecruitment.co.uk

6. COLLECTION AND PROCESSING OF DATA

The Company processes personal data relating to:

- Candidates.
- Temporary workers.
- Clients.
- Employees.
- Suppliers.

Personal data will only be processed where there is a lawful basis for doing so.

Employees must only collect information that is genuinely required for legitimate business purposes.

7. ACCESS CONTROLS

Access to information will be restricted to individuals who require it for legitimate business purposes.

Employees must:

- Use only authorised user accounts.
- Keep passwords confidential.
- Use multi-factor authentication where available.
- Never share login credentials.
- Log out of systems when appropriate.

Access rights may be amended or withdrawn at any time.

8. PASSWORDS AND AUTHENTICATION

Passwords must:

- Be kept confidential.
- Be sufficiently strong.
- Not be reused across multiple systems where possible.
- Not be written down in insecure locations.

Passwords must never be shared unless specifically authorised by a Director.

Any suspected compromise must be reported immediately.

9. PHYSICAL SECURITY

Employees must ensure that:

- Confidential documents are stored securely.
- Files are not left unattended.
- Screens are locked when unattended.
- Visitors are supervised appropriately.
- Personal information is not visible to unauthorised individuals.

A clear desk approach should be maintained wherever practical.

10. PAPER RECORDS

Paper records containing personal information must be:

- Stored securely.
- Accessed only by authorised personnel.
- Disposed of confidentially.

All documents containing personal or confidential information must be shredded or securely destroyed when no longer required.

Workshop Recruitment
Ashville House, 260-262 Havant Road, Drayton,
Portsmouth, Hampshire PO6 1PA England

Tel: 023 9232 4666
Fax: 023 9232 4777
Email: mail@workshoprecruitment.co.uk

11. ELECTRONIC INFORMATION SECURITY

Employees must not:

- Install unauthorised software.
- Download unapproved applications.
- Circumvent security controls.
- Disable security software.
- Use unauthorised cloud storage services.

Only approved systems and applications should be used for business purposes.

12. EMAIL SECURITY

Employees must take care when sending emails containing personal or confidential information.

Before sending emails employees should:

- Verify recipients.
- Check attachments carefully.
- Consider whether the information is necessary.
- Use secure methods where appropriate.

Misaddressed emails are a common cause of data breaches and must be avoided.

13. REMOTE WORKING

Employees working remotely must:

- Protect Company information.
- Lock devices when unattended.
- Avoid public access to confidential information.
- Exercise caution when using public Wi-Fi.
- Follow Company security procedures.

Business information should not be stored on personal devices unless specifically authorised.

14. CYBER SECURITY

All employees are responsible for supporting cyber security.

Employees must:

- Remain alert to phishing attempts.
- Report suspicious emails immediately.
- Avoid opening unexpected attachments.
- Follow security guidance issued by the Company.
- Report suspected cyber incidents immediately.

15. ARTIFICIAL INTELLIGENCE (AI)

The Company recognises the increasing use of artificial intelligence tools.

Employees must not upload the following into public AI systems without prior authorisation:

- Candidate CVs.
- Personal data.
- Employee information.
- Client information.
- Salary information.

Workshop Recruitment
Ashville House, 260-262 Havant Road, Drayton,
Portsmouth, Hampshire PO6 1PA England

Tel: 023 9232 4666
Fax: 023 9232 4777
Email: mail@workshoprecruitment.co.uk

• Commercially sensitive information.
All AI-generated outputs must be reviewed for accuracy before use.
Responsibility for decisions remains with the employee and not the AI system.

16. DATA RETENTION
Personal data will only be retained for as long as necessary.
The Company will maintain retention periods appropriate to:
• Candidates.
• Temporary workers.
• Employees.
• Clients.
• Financial records.
Information that is no longer required will be securely deleted or destroyed.

17. DATA SUBJECT RIGHTS
Individuals have rights including:
• Access to their information.
• Correction of inaccurate information.
• Erasure where applicable.
• Restriction of processing.
• Data portability.
• Objection to processing.
Any request relating to personal data must be referred immediately to a Director.

18. DATA BREACHES
Any actual or suspected data breach must be reported immediately to a Director.
Examples include:
• Lost devices.
• Misdirected emails.
• Unauthorised access.
• Lost paperwork.
• Cyber attacks.
• Malware incidents.
The Company will investigate breaches promptly and take appropriate action.

19. TRAINING AND AWARENESS
The Company will provide appropriate training and guidance regarding:
• Data protection.
• Information security.
• Cyber security.
• Data breach reporting.
• Safe handling of information.
Training records may be maintained.

20. RESPONSIBILITIES

Workshop Recruitment
Ashville House, 260-262 Havant Road, Drayton,
Portsmouth, Hampshire PO6 1PA England
Tel: 023 9232 4666
Fax: 023 9232 4777
Email: mail@workshoprecruitment.co.uk

The Directors have overall responsibility for:
• Compliance with data protection legislation.
• Information security management.
• Policy review.
• Incident response.
Managers and employees are responsible for complying with this policy and reporting concerns promptly.

21. MONITORING
The Company may monitor systems, devices and communications in accordance with applicable laws and Company policies.
Monitoring may be undertaken for:
• Information security.
• Regulatory compliance.
• Investigation of misconduct.
• Protection of Company assets.

22. BREACHES OF THIS POLICY
Failure to comply with this policy may result in disciplinary action.
Serious breaches may constitute gross misconduct including:
• Deliberate disclosure of confidential information.
• Serious data protection breaches.
• Misuse of personal data.
• Cyber security violations.
• Unauthorised access to systems.
The Company may also report breaches to relevant authorities where required.

23. POLICY REVIEW
This policy will be reviewed annually or sooner where necessary due to:
• Legislative changes.
• Regulatory guidance.
• Technological developments.
• Security incidents.

EMPLOYEE DECLARATION
I confirm that I have read, understood and agree to comply with the Company's Data Protection and Information Security Policy.

Employee Name: _____

Signature: _____

Date: _____

Workshop Recruitment
Ashville House, 260-262 Havant Road, Drayton,
Portsmouth, Hampshire PO6 1PA England

Tel: 023 9232 4666
Fax: 023 9232 4777
Email: mail@workshoprecruitment.co.uk