CONTROLLED POLICY

A03 – RECORDS MANAGEMENT, CONFIDENTIALITY AND DATA PROTECTION POLICY

Policy Reference	A03	**Version**	1.0
Policy Owner	PHSSL Staffing Limited	**Approved By**	Lade Awosika, Director
Approval Method	Approved electronically	**Approval Date**	September 2026
Review Date	September 2027	**Status**	Controlled Document
Applies To	All PHSSL Staffing Limited staff, workers and relevant contractors	**Supersedes**	New policy

1. Purpose

This policy explains how PHSSL Staffing Limited creates, uses, stores, shares, retains and disposes of records and personal information. It is designed to protect candidates, agency workers, employees, clients and other individuals while ensuring that recruitment and staffing records remain accurate, secure, accessible to authorised persons and available for legitimate business, legal and regulatory purposes.

2. Scope

This policy applies to directors, employees, recruitment and compliance staff, payroll and administrative staff, agency workers, temporary workers and relevant contractors. It covers paper and electronic records, recruitment platforms, email, payroll and timesheet information, personnel files, client records, communications and any other information processed on behalf of PHSSL Staffing Limited.

3. Policy Principles

- Personal information will be processed lawfully, fairly and transparently.
- Only information that is adequate, relevant and reasonably necessary will be collected.
- Records must be accurate, factual, legible and kept up to date where required.
- Access will be limited to authorised persons with a legitimate need to know.
- Personal information will be protected against unauthorised access, loss, alteration, disclosure or destruction.
- Information will not be retained for longer than necessary, subject to legal, contractual and regulatory requirements.
- Staff must report suspected confidentiality, privacy or information-security breaches immediately.

4. Legal and Regulatory Framework

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Employment Agencies Act 1973 and Conduct of Employment Agencies and Employment Businesses Regulations 2003, including applicable record-keeping requirements.
- Equality Act 2010.
- Immigration, Asylum and Nationality Act 2006 and applicable right-to-work requirements.
- Safeguarding and DBS requirements where applicable to a role.
- Employment, tax, payroll and other statutory record-keeping obligations applicable to PHSSL Staffing Limited.

5. Types of Records

Records held by PHSSL Staffing Limited may include:

- Candidate applications, CVs, employment histories and interview records.
- Identity and right-to-work evidence.
- DBS information and suitability/compliance records where relevant.
- References, qualifications, training and competency records.
- Key Information Documents, terms of engagement and assignment information.
- Client terms, vacancy information, bookings, placement records and communications.
- Timesheets, pay, holiday-pay, pension and payroll information.
- Absence, performance, complaints, incidents, safeguarding and disciplinary records where applicable.

- Contact details, emergency contacts and correspondence.
- Data-protection requests, consent records and information-security records.

6. Lawful Processing

PHSSL Staffing Limited will identify an appropriate lawful basis before processing personal information. Depending on the circumstances, processing may be necessary for a contract, steps requested before entering a contract, legal obligations, legitimate interests or another lawful basis. Where special-category or criminal-offence data is processed, an additional lawful condition will be identified and documented where required.

7. Data Minimisation

Staff must not collect information merely because it may be useful at some future point. Recruitment forms, compliance checks and client requests should be limited to information genuinely required for recruitment, placement, employment-business, safeguarding, payroll, legal or service-delivery purposes.

8. Accuracy and Record Quality

- Records must distinguish fact from opinion where this is relevant.
- Entries should be clear, dated and attributable to the person making them.
- Material errors must be corrected appropriately without misleading alteration of the historical record.
- Candidate and worker details should be updated when PHSSL becomes aware of relevant changes.
- Compliance expiry dates and other time-sensitive information must be monitored through suitable systems.

9. Confidentiality

Information obtained through recruitment and staffing work is confidential. Staff must not discuss candidates, workers, clients, assignments, incidents or personal circumstances with people who do not have a legitimate need to know.

- Do not leave confidential documents unattended in public or shared areas.
- Do not share passwords or allow unauthorised access to company systems.
- Check recipients carefully before sending email or attachments.
- Use approved systems and communication channels for confidential information.
- Do not disclose worker or candidate information to friends, relatives or other third parties without lawful authority.
- Confidentiality obligations continue after employment or engagement with PHSSL ends.

10. Sharing Candidate and Worker Information

Information may be shared with prospective or existing clients where this is necessary for recruitment, suitability assessment, placement or assignment administration and where there is a lawful basis. PHSSL will avoid sharing unnecessary personal details. Sensitive documentation such as identity documents, DBS information or health information must receive additional care and should not be routinely forwarded where verification or a limited confirmation is sufficient.

11. Client Information

Client contacts, staffing requirements, rates, contracts, commercial arrangements and other non-public information must be treated as confidential. Staff must not use client information for personal advantage or disclose it outside legitimate PHSSL business activities.

12. Special Category and Criminal-Offence Data

Health, disability, ethnicity, religion, trade-union membership and other special-category data require additional protection. Criminal-offence and DBS-related information must be handled in accordance with applicable law, DBS requirements and PHSSL procedures. Access must be strictly limited to those who require the information for an authorised purpose.

13. Equality Monitoring Information

Where equality-monitoring information is collected, it should be separated from selection decisions as far as practicable and used for legitimate monitoring and equality purposes. Recruitment decisions must not unlawfully discriminate on the basis of protected characteristics.

14. Right-to-Work and Identity Records

Right-to-work and identity checks must be completed and recorded in accordance with current legal requirements. Copies or electronic evidence must be securely retained for the required period and made available only to authorised persons or lawful authorities where appropriate.

15. DBS and Safeguarding Records

Where a role requires DBS or other safeguarding checks, PHSSL will record the information necessary to demonstrate appropriate checking and suitability decisions. Disclosure information will not be copied, retained or shared beyond what is lawful and necessary. Safeguarding information will be handled sensitively and disclosed only on a legitimate need-to-know basis.

16. Electronic Records and Cybersecurity

- Use company-approved devices, accounts, systems and storage wherever provided.
- Use strong passwords and multi-factor authentication where available.
- Lock screens when leaving devices unattended.
- Do not download confidential information to personal devices or removable media unless specifically authorised.
- Report lost devices, suspicious emails, malware, unauthorised access or other cyber concerns immediately.
- Follow backup, access-control and business-continuity arrangements established by PHSSL.

17. Paper Records

Paper files containing personal or confidential information must be stored securely when not in use. Documents should not be left in vehicles, reception areas or other locations where unauthorised persons may view them. Confidential waste must be securely destroyed.

18. Working Remotely

The same confidentiality and data-protection standards apply when working remotely. Staff must take reasonable steps to prevent household members, visitors or members of the public from seeing or hearing confidential information. Printed documents should be avoided unless necessary and must be stored and disposed of securely.

19. Email, Messaging and Telephone

- Confirm identity before discussing sensitive information by telephone.
- Use business email accounts for PHSSL business where available.
- Use blind-copy functions appropriately when emailing groups of unrelated recipients.
- Do not send confidential information through unapproved social-media or messaging accounts.
- Check attachments and recipients before transmission.
- Record important recruitment, assignment or compliance decisions in the appropriate business system rather than relying solely on informal messages.

20. Data Breaches

A personal-data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Any suspected breach must be reported to management immediately, even if the staff member believes the impact is minor. PHSSL will assess the incident, contain risks, preserve evidence and determine whether notification to the Information Commissioner's Office or affected individuals is required within applicable timescales.

21. Individual Information Rights

Individuals may have rights in relation to their personal information, including rights of access, correction, erasure, restriction, objection and data portability where applicable. Requests must be forwarded promptly to the person responsible for data protection and must not be ignored, deleted or answered informally without appropriate checks.

22. Subject Access Requests

A request for access to personal information does not need to use specific legal wording. Staff who receive a request that may be a subject access request must forward it promptly to management. Identity may need to be verified and information relating to other people may require careful review before disclosure.

23. Retention and Disposal

PHSSL Staffing Limited will maintain a retention schedule or other documented retention arrangements reflecting legal, contractual, regulatory and operational requirements. When records are no longer required, they will be securely deleted, anonymised or destroyed. A record subject to a complaint, legal claim, investigation, safeguarding matter or regulatory enquiry must not be destroyed simply because its normal retention period has expired.

24. Record Access and Audit Trail

Access permissions should reflect job responsibilities. Where systems provide audit logs, PHSSL may use them to monitor access, changes and compliance. Staff must never access a record out of curiosity or for a purpose unrelated to their duties.

25. Data Processors and Third-Party Systems

Where PHSSL uses payroll providers, recruitment platforms, cloud services or other processors, appropriate due diligence and contractual arrangements will be used as required. Personal information must not be transferred to an unapproved supplier simply for convenience.

26. International Transfers

Where personal information is transferred outside the United Kingdom, PHSSL will ensure that an appropriate lawful transfer mechanism and safeguards are in place where required.

27. Recruitment and Former Candidate Records

Information about unsuccessful candidates and former workers will be retained only for an appropriate period having regard to legal claims, regulatory requirements, legitimate business needs and any valid consent for future opportunities. People should not be kept indefinitely on recruitment databases without a justified retention basis.

28. Staff Responsibilities

- Follow this policy and related PHSSL procedures.
- Keep records accurate, timely and professional.
- Protect passwords, devices, files and confidential discussions.
- Share information only with authorised persons for legitimate purposes.
- Report data breaches, lost records and confidentiality concerns immediately.
- Complete required data-protection and information-security training.
- Seek management advice when unsure whether information may lawfully be disclosed.

29. Management Responsibilities

- Maintain appropriate privacy notices, retention arrangements and information-security controls.
- Ensure staff receive appropriate training and access only to information needed for their roles.
- Respond appropriately to data-subject requests and data breaches.
- Maintain oversight of third-party processors and systems.
- Audit records and address identified weaknesses.
- Ensure recruitment, compliance and payroll record keeping meets applicable legal and contractual requirements.

30. Related PHSSL Staffing Policies

- A01 Governance and Quality Assurance Policy.
- A02 Business Continuity and Emergency Planning Policy.
- A04 Complaints, Concerns and Service Feedback Policy.
- B01 Safeguarding Adults Policy.

- B02 Safeguarding Children and Young People Policy.
- B03 Whistleblowing / Speaking Up Policy.
- C01 Recruitment, Selection and Safer Employment Policy.
- C02 DBS, Right to Work, References and Pre-Employment Checks Policy.
- D03 Placement, Booking, Allocation and Cancellation Policy.
- D05 Timesheets, Pay, Holiday Pay and Payroll Policy.

31. Monitoring and Review

Compliance will be monitored through file audits, access controls, incident and breach reviews, recruitment and compliance audits, staff supervision and governance processes. This controlled policy will be reviewed at least annually, or sooner following significant legal, regulatory, technological or organisational change, a serious data incident, audit findings or identified learning.

Approved by	Lade Awosika
Position	Director
Approval method	Approved electronically
Approval date / next review	September 2026 / September 2027