

Pegasus Healthcare – Privacy Policy

Version	Version 2.0	Applies to	Website visitors, candidates, agency workers, office staff, client contacts, people supported by our workers, referees and emergency contacts
Effective date	22/10/2026	Replaces	Privacy Policies on the website Legal page (last updated 18 December 2021)
Next review date	22/10/2027	ICO registration	ZB270379
Owner	Simon Shinwell, Managing Director (Data Protection Lead)	Contact	simon@pegasuscare.co.uk · 0141 280 8188

Pegasus Healthcare Solutions Limited · Company no. SC707859 · Registered office: 145 St Vincent Street, Glasgow · Trading address: 53 Bothwell Street, Glasgow G2 6TS · Registered with the Care Inspectorate as a nurse agency (CS2022000069)

1. Privacy at a glance

This privacy policy (our privacy notice) explains how Pegasus Healthcare Solutions Limited ("Pegasus Healthcare", "we", "us", "our") collects, uses, shares and protects personal data. It is written in layers: this first section is a short summary, section 3 shows which sections apply to you, and the later sections give the full detail.

In short	What it means for you
Who we are	A care staffing agency (employment business) in Glasgow, supplying nurses, carers and support workers to care homes, care at home services, councils, the NHS and other organisations. We are the controller of the personal data described in this policy.
What we collect	The information we need to recruit, check, place, pay and support workers; to run our client accounts; to answer enquiries; and to keep the people our workers support safe.
Why	To meet our contracts, to comply with the law (for example right-to-work, PVG, tax, Care Inspectorate and SSSC requirements), to protect vulnerable people, and for our legitimate business interests.
Sensitive data	We handle health information and criminal record information (through the PVG scheme run by Disclosure Scotland) only where the law allows it, with extra safeguards.
Who sees it	Our own team, our clients (only what they need), regulators and public bodies where the law requires it, and service providers that work for us under contract. We never sell personal data.
How long	Unsuccessful candidates 6 months; workers 2 years after their last shift; payroll and tax records 6 years. See section 14.
Your rights	You can ask for a copy of your data, ask us to correct it, object to some uses and, in some cases, ask us to delete or restrict it. See section 16.
Concerns	Contact us first and we will acknowledge your complaint within 30 days. You can then complain to the Information Commissioner's Office (ICO). See section 18.

2. Who we are and how to contact us

Item	Details
Controller	Pegasus Healthcare Solutions Limited, a company registered in Scotland, company number SC707859. "Pegasus Healthcare" and "Pegasus Healthcare Solutions" are our trading names.
Registered office	145 St Vincent Street, Glasgow G2 5JF
Trading address	2nd Floor, 53 Bothwell Street, Glasgow G2 6TS
ICO registration	ZB270379 (Information Commissioner's Office register of fee payers)
Care Inspectorate	Registered with the Care Inspectorate, registration number CS2022000069
Data Protection Lead	Simon Shinwell, Managing Director – simon@pegasuscare.co.uk – 0141 280 8188. Simon is responsible for data protection at Pegasus Healthcare, including rights requests and data protection complaints. We keep under review whether a statutory Data Protection Officer is required; at the date of this policy our Data Protection Lead carries out this role.
Registered Manager	Ruth Shinwell, Director and Registered Manager, leads on care quality and safeguarding.
General contact	helpdesk@pegasuscare.co.uk · info@pegasuscare.co.uk · 0141 280 8188 (24 hours)

You can ask for this policy in another format (for example large print or a paper copy) by contacting us using any of the details above. You do not need to write to our registered office.

3. Who this policy covers and how it is organised

Find the group, or groups, that apply to you. Many people fall into more than one group – for example, an agency worker may also be a website visitor and an emergency contact for a colleague.

Your relationship with us	Read
A visitor to pegasuscare.co.uk , or someone who contacts us with an enquiry	Sections 4 and 5 (including cookies)
A candidate applying to work with us, or an agency worker (nurse, carer or support worker)	Section 6
A member of our office team	Section 7
A contact at a client or hiring organisation (care home, care at home provider, council, NHS board, health and social care partnership or other hirer)	Section 8
A person supported by one of our workers, or their family or representative	Section 9
A referee	Section 10
An emergency contact or next of kin	Section 11
Everyone	Sections 12 to 19 (sharing, international transfers, retention, security, your rights, automated decisions, complaints and changes)

Our lawful bases explained

Data protection law – the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), both as amended by the Data (Use and Access) Act 2025 (DUAA) – only allows us to use personal data where we have a "lawful basis". These are the bases we rely on in this policy:

Lawful basis	What it means
Contract	We need the data to enter into or perform a contract with you – for example your contract for services as an agency worker, a contract of employment, or a client agreement (Article 6(1)(b) UK GDPR).
Legal obligation	The law requires us to use the data – for example right-to-work checks, PVG checks, tax and National Minimum Wage records, the Conduct of Employment Agencies and Employment Businesses Regulations 2003, and Care Inspectorate requirements (Article 6(1)(c)).
Recognised legitimate interest	A purpose that the DUAA treats as legitimate without a separate balancing test: safeguarding vulnerable individuals (children and adults at risk), detecting or preventing crime, responding to emergencies, national or public security, and responding to a request from a public body that confirms it needs the data for its public task (Article 6(1)(ea) and Annex 1 UK GDPR).
Legitimate interests	We need the data for our business or for a third party's legitimate interests, and we have checked that these are not overridden by your interests and rights – for example matching workers to shifts, quality assurance, keeping in touch with clients, and defending legal claims (Article 6(1)(f)). You can object to this (section 16).
Vital interests	We need to use the data to protect someone's life, for example in a medical emergency (Article 6(1)(d)).
Consent	You have given clear consent for a specific purpose, such as non-essential cookies or optional marketing. You can withdraw consent at any time. We rarely rely on consent for workers or staff, because of the imbalance of power in a working relationship.

Health information is **special category data** and criminal record information (including PVG scheme records) is **criminal offence data**. For these we also need a condition under Article 9 or Article 10 UK GDPR and Schedule 1 to the DPA 2018. Where Schedule 1 requires it, we keep an Appropriate Policy Document explaining how we protect this data and how long we keep it.

4. Website visitors and enquirers

This section covers people who visit pegasuscare.co.uk, use our contact forms, phone or email us, or follow links to our job board, candidate app or client portal.

Topic	Details
What we collect	Technical data that any website receives, such as your IP address, browser and device type, the pages you visit and the time of your visit (in our website host's server logs). If you contact us: your name, email address, phone number, the subject of your enquiry and anything you choose to tell us. If you phone us: your number, the details of your call and a call recording (calls are recorded for security, monitoring and training, and callers are told this).
Where it comes from	Directly from you and from your device.
Why we use it	To run and secure our website; to answer your enquiry; to pass a job or registration enquiry into our recruitment process; to pass a service enquiry to our client team; and to keep a record of calls for security, training, quality and safeguarding.

Topic	Details
Lawful basis	Legitimate interests (running a secure website, answering enquiries and keeping call records); contract, where you ask us to take steps before entering into a contract (for example registering as a candidate or client); legal obligation or a recognised legitimate interest where a call or message raises a safeguarding or crime concern.
Sensitive data	We do not ask for health or criminal record information through our general contact forms. Please do not include it. If you do share it (for example in a call about a concern), we use it only for the purpose for which you shared it and under the conditions in sections 6 and 9.
Shared with	Our website host and IT/email provider, our telephony provider, and – for job and app enquiries – the provider of our candidate app and booking portal.
International transfers	Some website and IT services, including web fonts loaded from a third-party provider's servers, may involve your IP address being processed outside the UK. See section 13.
How long	Enquiries that do not lead to a working relationship: up to 2 years from our last contact. Server logs: kept by our host for a short period for security, then deleted. Call recordings: kept only as long as needed for security, monitoring and training, then deleted, unless a recording is needed for a complaint, safeguarding concern, investigation or claim, in which case it is kept with that record (section 14).
Automated decisions	None.
Marketing	We only send electronic marketing to individuals with consent, or where the law allows us to contact existing customers or business contacts. Every message includes a simple way to opt out, and you can opt out at any time by contacting us.

Our website links to other sites, such as social media sites, the Care Inspectorate and app stores. Those organisations have their own privacy policies, and we are not responsible for how they use your data.

5. Cookies and similar technologies

Cookies are small files placed on your device when you visit a website. The Privacy and Electronic Communications Regulations 2003 (PECR), as amended by the DUAA, say that we must tell you about cookies and similar technologies, and ask for your consent unless an exemption applies. The same rules apply to similar technologies used by mobile apps.

Cookies we use

Type	Purpose	Consent
Strictly necessary	Cookies set by our website software (our content management system and its page-builder and form plugins) to deliver pages, keep forms secure and prevent spam or misuse.	Not needed – these are exempt because the website cannot work properly without them.
Third-party content	Our website shows the Care Inspectorate's grading widget and loads web fonts from a third-party provider's servers. These services receive your IP address so they can deliver the content, and may set their own cookies.	We will ask for consent before loading any third-party content that sets non-essential cookies, or host the content ourselves so that no third-party cookies are set.

Type	Purpose	Consent
Analytics (statistics)	At the date of this policy our website does not use analytics cookies.	If we add them, we will use them only to understand how the website is used and improve it, give clear information, and offer a simple, free way to opt out, as the DUAA exemption for statistical purposes requires; otherwise we will ask for consent.
Preferences	Cookies that remember choices such as display settings.	Exempt under the DUAA where used only to remember your preferences, as long as we tell you and you can easily opt out.
Advertising and tracking	We do not use advertising, social media tracking or cross-site tracking cookies.	These would always need your consent before being set.

Managing cookies

You can block or delete cookies through your browser settings. Blocking strictly necessary cookies may stop parts of the website, such as forms, from working. Where we ask for consent, you can change your choice at any time, and it will be as easy to withdraw consent as it was to give it.

Our candidate app and portal

Our candidate app and our booking portal for clients and workers use similar technologies to keep you logged in, keep your account secure and send notifications. These are strictly necessary for the service you have asked for. Where a feature uses your device's location (for example to confirm attendance at a shift), your device will ask for your permission first, and you can turn it off in your device settings.

6. Candidates and agency workers

This section covers people who apply to work with us and people we register and supply as agency workers. Our agency workers are engaged under a **contract for services** (they are free to accept or refuse assignments and have worker status); they are not employees and we do not use zero-hours contracts of employment. Office staff should read section 7.

Topic	Details
What we collect	Identity and contact: name, previous names, address history, date of birth, phone, email, photograph (for your staff profile and ID badge). Recruitment: CV or application, employment history and gaps, qualifications and training certificates, interview notes, telephone screening answers, references (section 10). Right to work: passport, visa or eVisa share code result, birth or marriage certificate, Identity Service Provider check result, and any work restrictions. Registration: SSSC or NMC registration details, conditions, revalidation dates and register checks. PVG: PVG scheme membership, Level 2 disclosure information, a criminal record self-declaration and, where you have lived or worked abroad, overseas criminal record certificates. Health: a confidential health questionnaire after a conditional offer, fitness for work and reasonable adjustments, sickness absence. Work and pay: availability, shifts worked, timesheets, holiday, National Insurance number, tax code and HMRC starter checklist, bank details, pension auto-enrolment information, Working Time Regulations opt-out (if you choose to sign one). Training: e-learning results and certificates on our e-learning platform, practical training attendance. Conduct and quality: client feedback, incidents, complaints, concerns, supervision, investigations and outcomes. Equality monitoring: only if you choose to give it. Emergency contact details (section 11).

Topic	Details
Where it comes from	You; your referees; Disclosure Scotland; the SSSC and NMC online registers; the Home Office online checking service and certified Identity Service Providers; overseas criminal record authorities; HMRC; our clients (feedback, timesheets and incident reports); our HR system, e-learning platform and candidate app; and, where a concern is raised, council social work services, Police Scotland, the Care Inspectorate, the SSSC or the NMC.
Why we use it	To assess your application; carry out the checks the law requires before you work with vulnerable people; register and induct you; train you; match you to suitable shifts and tell clients about you; pay you and keep pay, tax and working time records; manage holiday, absence and reasonable adjustments; monitor quality, conduct and compliance (including expiry of PVG membership, training and registration); deal with complaints, incidents and safeguarding concerns; make referrals to regulators where required; manage insurance and legal claims; and meet our legal duties as an employment business and registered care service.
Lawful basis	Contract – your contract for services and the steps before it. Legal obligation – right-to-work checks (Immigration, Asylum and Nationality Act 2006); PVG checks (Protection of Vulnerable Groups (Scotland) Act 2007 and Disclosure (Scotland) Act 2020); the Conduct of Employment Agencies and Employment Businesses Regulations 2003; HMRC, National Minimum Wage, working time, statutory sick pay and pension auto-enrolment duties; Care Inspectorate requirements for registered care services; SSSC and NMC duties. Recognised legitimate interest – safeguarding vulnerable individuals and preventing or detecting crime. Legitimate interests – matching you to shifts, quality assurance, keeping our candidate pool up to date, managing our insurance and defending claims.
Article 9 condition (health and equality data)	Employment, social security and social protection (Article 9(2)(b) and Schedule 1, Part 1, paragraph 1 DPA 2018); assessing working capacity as part of health or social care (Article 9(2)(h) and paragraph 2); equality of opportunity monitoring (Schedule 1, Part 2, paragraph 8); safeguarding of children and individuals at risk (paragraph 18); and establishing, exercising or defending legal claims (Article 9(2)(f)).
Article 10 condition (criminal records via PVG)	Criminal record information is processed under Article 10 UK GDPR and section 10(5) DPA 2018, relying on Schedule 1, Part 1, paragraph 1 (employment, linked to our legal duties under the PVG Act and the Disclosure (Scotland) Act 2020), Part 2, paragraph 18 (safeguarding of children and individuals at risk) and Part 3, paragraph 33 (legal claims). We handle disclosure information in line with the Scottish Ministers' Code of Practice under the Disclosure (Scotland) Act 2020 and our Recruitment of Ex-Offenders Policy: stored securely, seen only by those who need it, and never used for any other purpose. Having a conviction does not automatically prevent you from working with us.
Shared with	Clients you are proposed to or placed with – only what they need for a safe booking (name, role, training and competence, confirmation of PVG membership, registration status and right-to-work confirmation where required); full disclosure certificates, health information and ID documents are not shared unless a specific lawful basis applies. Disclosure Scotland; the SSSC and NMC; the Home Office; HMRC; our payroll provider and pension provider; our HR system provider and e-learning provider; the provider of our candidate app and booking portal; our IT/email and telephony providers; practical training providers; the Care Inspectorate; council social work and Police Scotland where there is a safeguarding or crime concern; our insurer and insurance brokers; legal and professional advisers; and courts or tribunals where required. See section 12.
International transfers	Overseas criminal record checks and references from overseas employers involve contacting organisations in other countries. Some service providers may also process data outside the UK. See section 13.

Topic	Details
How long	Unsuccessful candidates: 6 months after the recruitment decision. Agency workers: 2 years after they last worked with us. This covers personnel, registration, training, reference, right-to-work and working time records, and the PVG check record (type, date, reference, outcome and decision). Payroll, tax and pay records: 6 years. See section 14.
Automated decisions	We do not make decisions about you based solely on automated processing that have a legal or similarly significant effect. Our systems may automatically flag or pause booking when a compliance item (for example PVG membership, SSSC or NMC registration, right to work or mandatory training) has expired, but a member of our team reviews every case and you can ask us to look at it again. See section 17.
If you do not provide data	Much of the information above is required by law or by your contract. If you do not provide it, we may not be able to register you or offer you work.

7. Office staff

This section covers people who work in our office team under a contract of employment, and applicants for office roles.

Topic	Details
What we collect	Identity and contact details; application, interview and reference information; right-to-work checks; PVG information where the role requires it; contract, salary, bank, tax, National Insurance and pension details; working hours, holiday and absence (including family leave); health information for sickness, fitness for work and reasonable adjustments; training records on our e-learning platform; appraisal, performance, conduct, grievance and disciplinary records; IT, phone and email records created through work, including call recordings; emergency contacts; equality monitoring information only if you choose to give it.
Where it comes from	You; referees; Disclosure Scotland; the Home Office; HMRC; your doctor or an occupational health adviser (only with your agreement where the law requires it); our HR system and e-learning platform; colleagues and clients (for example feedback or complaints).
Why we use it	To recruit you; manage your employment, pay, pension and benefits; meet our legal duties as an employer; manage performance, conduct, absence and wellbeing; train you; keep our systems secure; and deal with disputes and claims.
Lawful basis	Contract (your contract of employment); legal obligation (employment, tax, right-to-work, health and safety, pension and PVG law); legitimate interests (managing our business, IT security and quality); recognised legitimate interest (safeguarding and preventing crime).
Article 9 and 10 conditions	As for agency workers in section 6: employment and social protection; assessing working capacity; equality monitoring; safeguarding; legal claims. Criminal record information only where the role requires a PVG check, under the same conditions.
Shared with	Our HR system provider, our e-learning provider, our payroll and pension providers, HMRC, Disclosure Scotland, IT/email and telephony providers, our insurer and brokers, legal and professional advisers, and regulators where required.
International transfers	See section 13.
How long	Office staff records: 6 years after employment ends. Right-to-work copies: 2 years after employment ends. Unsuccessful applicants: 6 months after the recruitment decision. See section 14.
Automated decisions	None (section 17).

8. Clients and hiring organisations

This section covers individual contacts at organisations that use our services or that we approach about our services – for example care home managers, care at home providers, council and health and social care partnership officers, NHS staff and procurement contacts. Information about the organisation itself is not personal data, but information about its staff is.

Topic	Details
What we collect	Names, job titles, work email addresses and phone numbers (including emergency and out-of-hours numbers), the organisation's address, booking requests and instructions, timesheet authorisations, feedback and complaints, invoices and payment details, portal log-in details, and records of our communications.
Where it comes from	You and your colleagues; our client portal; public sources such as your organisation's website, the Care Inspectorate's register of care services and procurement portals.
Why we use it	To set up and manage your account; take and fill bookings; send timesheets and invoices; resolve queries, concerns and complaints; report incidents and safeguarding concerns; review service quality; meet our contract and framework obligations; and tell you about our services.
Lawful basis	Legitimate interests (managing our relationship with your organisation and promoting our services to business contacts); contract (where you are a sole trader or partnership); legal obligation (records we must keep under the 2003 Regulations, tax and Care Inspectorate requirements).
Shared with	Our IT/email provider, the provider of our booking portal, our accountants and auditors, our insurer and brokers, legal advisers, and regulators where required.
International transfers	See section 13.
How long	Client account, booking, timesheet and invoice records: 6 years after the relationship ends. Business development contacts: until you ask us to stop, reviewed at least every 2 years.
Your choices	You can ask us to stop sending marketing at any time. Under PECR we only send marketing emails to individuals (including sole traders and some partnerships) with consent or under the "soft opt-in" for existing customers, and every message includes a simple opt-out.
Automated decisions	None (section 17).

9. People supported by our workers

Our workers support adults – and sometimes children – in care homes, in their own homes and in hospitals and other services. Day-to-day care records (such as care plans, medication records and daily notes) belong to the client organisation, which is the controller of them. Our workers must follow the client's confidentiality and data protection rules as well as ours. Pegasus Healthcare is the controller only of the limited records we create or receive ourselves, described below.

Topic	Details
What we collect	Your name and the service or address where you were supported; the date, time and details of an incident, accident, concern, complaint or compliment; relevant health and care information (for example an injury, a medication error or a change in condition); safeguarding information; and the outcome of any investigation. Sometimes we also hold the names and contact details of your family or representative.

Topic	Details
Where it comes from	Our workers' incident and concern reports; the client organisation; you or your family or representative; council social work services; the NHS; Police Scotland; and the Care Inspectorate.
Why we use it	To keep you and others safe; report and respond to adult or child protection concerns, including under the Adult Support and Protection (Scotland) Act 2007 and child protection procedures; notify the Care Inspectorate where required; carry out the organisational duty of candour; investigate complaints and incidents; take action about a worker's conduct or practice, including referrals to Disclosure Scotland, the SSSC or the NMC; and manage insurance and legal claims.
Lawful basis	Legal obligation (Care Inspectorate requirements for registered care services; the duty of candour under the Health (Tobacco, Nicotine etc. and Care) (Scotland) Act 2016; PVG referral duties); recognised legitimate interest (safeguarding vulnerable individuals; preventing or detecting crime; responding to a public body, such as a council carrying out an adult protection inquiry, that confirms it needs the information for its public task); vital interests (in an emergency); legitimate interests (handling complaints and defending claims).
Article 9 and 10 conditions	Provision of health or social care (Article 9(2)(h) and Schedule 1, Part 1, paragraph 2 DPA 2018); safeguarding of children and individuals at risk (Schedule 1, Part 2, paragraph 18); vital interests where you cannot give consent (Article 9(2)(c)); and legal claims (Article 9(2)(f)). If a report includes information about an alleged offence, we rely on the safeguarding and legal claims conditions in Schedule 1.
Shared with	The client organisation responsible for your care; council social work services and health and social care partnerships; the NHS; Police Scotland; the Care Inspectorate; Disclosure Scotland, the SSSC or the NMC (where a worker is referred); the Procurator Fiscal or courts where required; and our insurer, brokers and legal advisers. We share only what is necessary.
International transfers	We do not intend to transfer this information outside the UK, other than through service providers described in section 13.
How long	Incident, safeguarding, complaint and duty of candour records: 6 years after the matter is closed (for a child, until their 25th birthday if later). Accident and RIDDOR records: at least 3 years. See section 14.
Your rights	You, or someone acting for you (such as a welfare guardian or attorney, or a parent for a young child), can use the rights in section 16. Some rights may be limited where the law allows – for example where releasing information could cause serious harm or would reveal information about another person.
Automated decisions	None (section 17).

10. Referees

Topic	Details
What we collect	Your name, job title, organisation, work contact details, your relationship to the candidate, the reference you give, and a note of any phone call to verify it.
Where it comes from	The candidate who named you, and you.
Why we use it	To obtain and verify references, as the 2003 Regulations, Care Inspectorate safer recruitment guidance and our Recruitment Policy require.

Topic	Details
Lawful basis	Legal obligation (regulation 22 of the 2003 Regulations) and legitimate interests (safe recruitment).
Shared with	Kept on the candidate's file and seen only by people involved in the recruitment decision, and by regulators or auditors checking our recruitment. We request references through a secure online portal or your verified work email address.
International transfers	If you are based outside the UK, we will contact you where you are. See section 13.
How long	With the candidate's file: 6 months after the recruitment decision if the candidate is not engaged, or 2 years after they last worked with us if they are.
Your rights	You can use the rights in section 16. The candidate may ask to see their reference. We will consider any request for confidentiality, but references may sometimes be disclosed to the candidate where the law requires it.
Automated decisions	None.

11. Emergency contacts and next of kin

Topic	Details
What we collect	Your name, relationship to the worker or staff member, and phone number.
Where it comes from	The worker or staff member who named you. We ask them to tell you that they have given us your details and to point you to this policy.
Why we use it	Only to contact you in an emergency, such as an accident or illness at work, or if we cannot reach the worker and are concerned for their safety.
Lawful basis	Legitimate interests (being able to act in an emergency) and vital interests (in a medical emergency).
Shared with	Not shared, except with emergency services where necessary.
How long	Deleted when the worker gives us a new contact or when their engagement or employment ends, unless it forms part of a record of an incident.
International transfers and automated decisions	None.

12. Who we share personal data with

We share personal data only where we have a lawful basis, and only what is needed. We never sell personal data.

Recipient	Why
Clients and hiring organisations	To propose and place workers safely, and to manage bookings, timesheets, incidents and complaints.
Disclosure Scotland	PVG scheme applications, membership updates and referrals required by the PVG Act.
Scottish Social Services Council (SSSC) and Nursing and Midwifery Council (NMC)	Registration checks and fitness to practise referrals.

Recipient	Why
Care Inspectorate	Notifications, inspections and information requests made under its regulatory powers.
Council social work services, health and social care partnerships, NHS and Police Scotland	Adult and child protection concerns, inquiries and investigations, including under the Adult Support and Protection (Scotland) Act 2007.
Home Office and HMRC	Right-to-work checks; pay, tax and National Insurance reporting.
Service providers (processors)	our HR system provider; our e-learning provider; the provider of our candidate app and booking portal; our payroll provider; our pension provider; our IT, email, telephony and website hosting providers; certified Identity Service Providers; practical training providers. They act on our instructions under written contracts that meet Article 28 UK GDPR.
Insurer and brokers	Our insurer and insurance brokers, for cover, renewals, incidents and claims.
Professional advisers	Legal advisers, accountants and auditors.
Courts, tribunals, the Procurator Fiscal and other public bodies	Where the law requires it, or where a public body confirms it needs the information for its public task.
A future owner of our business	If we sell or restructure our business, personal data may be transferred to the new owner, who must protect it in the same way.

13. International transfers

We aim to keep personal data in the UK. Some of our service providers (for example cloud email, IT, app and HR system providers, and web fonts loaded from a third-party provider's servers) may store or access data outside the UK, and overseas criminal record checks and overseas references involve contacting organisations abroad.

When personal data is transferred outside the UK, we make sure it is protected by one of the safeguards in UK data protection law, as amended by the DUAA:

- the destination is covered by UK "data protection test" regulations (often called adequacy regulations), such as the European Economic Area and countries or organisations recognised by the UK Government, including those certified under the UK Extension to the EU-US Data Privacy Framework; or
- the transfer is covered by appropriate safeguards, such as the ICO's International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses; or
- a specific exception applies, for example where you have asked us to obtain an overseas criminal record certificate or reference as part of your application.

You can ask our Data Protection Lead for more information about the safeguards that apply to any transfer.

14. How long we keep personal data

We keep personal data only as long as we need it, and never for less than the law requires.

Record	Retention
Unsuccessful candidates	6 months after the recruitment decision
Agency worker personnel, registration, training and reference records	2 years after they last worked with us
Office staff personnel and training records	6 years after employment ends

Record	Retention
Right-to-work check copies	2 years after the person last worked with us
Payroll, tax and pay records	6 years
Working time and holiday records	2 years (Working Time Regulations 1998)
Records under the Conduct of Employment Agencies and Employment Businesses Regulations 2003	At least 1 year from creation or last supply, and in practice with the personnel file
PVG and Disclosure Scotland checks	Record of the check (type, date, reference, outcome and decision): 2 years after the worker last worked with us. Disclosure information itself: only as long as needed to make and record the decision.
Accident and RIDDOR records	At least 3 years
Incident, safeguarding, complaint and duty of candour records	6 years after the matter is closed (for a child, until their 25th birthday if later)
Client account, booking, timesheet and invoice records	6 years after the relationship ends
Business development contacts	Until you opt out; reviewed at least every 2 years
Website and email enquiries	Up to 2 years from our last contact, unless the enquiry leads to a working relationship
Call recordings	Only as long as needed for security, monitoring and training, unless needed for a complaint, safeguarding concern, investigation or claim
Emergency contacts	Until replaced, or until the engagement or employment ends

When the retention period ends, we securely delete electronic records and shred paper records, or anonymise information so it no longer identifies anyone.

15. How we keep personal data secure

- Access to personal data is limited to people who need it for their role, using strong passwords and multi-factor authentication on our systems.
- Our information is protected by encryption and firewalls, and backed up in more than one location so authorised staff can access it securely if our office is unavailable.
- Paper records are kept in locked storage and shredded securely when no longer needed.
- Our staff and workers complete data protection and confidentiality training on our e-learning platform at induction and at least every two years.
- Our service providers are assessed for security and work under written contracts.
- If a personal data breach is likely to result in a risk to people's rights and freedoms, we report it to the ICO without undue delay and, where feasible, within 72 hours; if there is a high risk to you, we will tell you without undue delay.

16. Your rights

You have the following rights. Some apply only in certain circumstances, and some may be limited where an exemption in the DPA 2018 applies (for example to protect other people or to avoid prejudicing the prevention or detection of crime).

Right	What it means
To be informed	To be told how we use your data – this policy does that.
Access	To ask for a copy of your personal data and information about how we use it (a subject access request).
Rectification	To have inaccurate data corrected and incomplete data completed.
Erasure	To ask us to delete your data, for example where we no longer need it. We may not be able to delete data that we must keep by law.
Restriction	To ask us to limit how we use your data while a concern is looked into.
Objection	To object to our use of your data based on legitimate interests (including recognised legitimate interests), and to object at any time to direct marketing, which we will then stop.
Data portability	To receive data you gave us, in a commonly used electronic format, where we use it on the basis of contract or consent by automated means.
Automated decisions	Rights relating to significant decisions made solely by automated means (section 17).
Withdraw consent	Where we rely on consent, you can withdraw it at any time. This does not affect anything we did before you withdrew it.

How to make a request

You can make a request in any way you like – by email to simon@pegasuscare.co.uk or helpdesk@pegasuscare.co.uk, by phone on 0141 280 8188, in writing, or by speaking to any member of our team. You do not need to use a particular form or write to our registered office.

- We will respond without undue delay and within one month. We can extend this by up to two further months for complex or numerous requests, and we will tell you if we do.
- If we need information to confirm your identity or to understand your request, the time limit pauses until we receive it.
- When responding to a subject access request we carry out reasonable and proportionate searches for your data.
- Requests are free, unless they are manifestly unfounded or excessive, in which case we may charge a reasonable fee or refuse, and we will explain why.

17. Automated decision-making and AI

We do not make decisions that have a legal or similarly significant effect on anyone based solely on automated processing, including profiling. People make decisions about recruitment, placements, pay and conduct.

Our systems help us by sorting information and flagging items – for example, showing workers who are available and compliant for a shift, or pausing bookings when PVG membership, registration, right to work or mandatory training has expired. A member of our team reviews these flags.

If we introduce automated tools, including artificial intelligence, that make significant decisions about people, we will assess the risks first (including a data protection impact assessment where required), update this policy and tell the people affected. Under the DUAA you would then have the right to be told about the decision, to make representations, to have a person review the decision and to contest it. We will not make solely automated significant decisions using health or criminal record information.

18. Complaints – tell us first, then the ICO

If you are unhappy with how we have used your personal data, please complain to us first. Since 19 June 2026, section 164A of the DPA 2018 (inserted by the DUAA) gives you the right to complain directly to us, and we must handle your complaint properly.

Step	What happens
1. Contact us	Email simon@pegasuscare.co.uk or helpdesk@pegasuscare.co.uk , phone 0141 280 8188, write to us at 2nd Floor, 53 Bothwell Street, Glasgow G2 6TS, or use the electronic complaint form on our online portal.
2. Acknowledgement	We will acknowledge your complaint within 30 days of receiving it.
3. Investigation	Our Data Protection Lead will look into your complaint without undue delay, keep you informed of progress, and tell you the outcome.
4. The ICO	If you are not satisfied with our response, you can complain to the Information Commissioner's Office: ico.org.uk/make-a-complaint , helpline 0303 123 1113. ICO Scotland: Queen Elizabeth House, Sibbald Walk, Edinburgh EH8 8FT, telephone 0303 123 1115, scotland@ico.org.uk . The ICO will usually expect you to have raised your complaint with us first.

Complaints about the quality of care or a worker's practice, rather than about personal data, are handled under our Complaints Policy. You can also complain to the Care Inspectorate at any time.

19. Changes to this policy

We review this policy at least once a year, and sooner if the law, ICO guidance or the way we use personal data changes. The current version is always available on our website and from our office. If we make a significant change – for example a new purpose, a new type of data or a new category of recipient – we will tell the people affected before the change takes effect, through our candidate app, our HR system, email or our website, as appropriate. Each version shows its version number and effective date on the first page.

What changed in this version

This version replaces the Privacy Policies on our website's Legal page, last updated on 18 December 2021. It brings them up to date with the UK GDPR, the DPA 2018 and the DUAA, PECR cookie rules and the ICO's guidance on privacy notices. It now covers every group of people whose data we handle; explains our lawful bases and the conditions for health and criminal record information; adds retention periods, international transfers, automated decision-making and a full list of rights; explains the new complaints process; and adds a cookies section.