Staff Privacy Notice

October 2024

Version No	Date Issued	Update Details	Owner	Approved By	Policy Number
v4.0	February 2022	Policy in previous format.	Company Secretary	The Board	POL-026
v5.0	April 2023	Policy finalised following revision and review of previous policy, amendments and change of format.	Company Secretary	The Board	POL-026
v5.1	June 2023	Policy amended to refer to occupational health processing by RPS	Company Secretary	The Board	POL-026
v5.2	January 2024	Policy amended to include processes identified by the Record of Processing Activity.	Company Secretary	The Board	POL-026
v5.3	October 2024	Reference to telephony support services processing by Onecom Ltd added	Company Secretary	The Board	POL-026

Staff Privacy Notice

Clancy Group Holdings Limited and its and its associated companies Clancy Plant Limited and Clancy Docwra Limited (Clancy or we) are committed to protecting your personal information, as well as being transparent about the personal information collected, obtained and disclosed about you.

This Privacy Notice ("Notice") will inform you as to how we look after your personal data during and after your employment and to ensure that all of our data protection obligations are met.

Notice

This Notice describes the categories of personal data that we collect, how we use your personal data, how we secure your personal data, when we may disclose your personal data to third parties, and when we may transfer your personal data outside of your home jurisdiction.

This Notice also describes your rights regarding your personal data. We will only process your personal data in accordance with this Notice unless otherwise required by applicable law.

This Notice is reviewed annually by our Data Protection and Compliance Officer ("DPCO") or nominated person and will be monitored for compliance by the DPCO, and line managers/supervisors within their own area of responsibility. Routine audits will be carried out annually and may also include random and scheduled inspections by the DPCO. If you have any questions about this Notice, including any requests to exercise your legal rights, please contact our DPCO using the details set out below.

This Notice does not form part of any contract of employment, and we may amend it at any time.

Controller: This Notice is issued on behalf of the Clancy Group so when we mention "Clancy", "we", "us" or "our" in this Notice, we are referring to the relevant company in the Clancy Group responsible for processing your data.

This Notice applies to all employees working for Clancy at all levels and applies to any temporary and contracted individuals, consultants, seconded employees, agency workers, working for or on behalf of Clancy (referred to as "you" in this Notice).

The data we collect about you

We take steps to ensure that the personal data that we collect about you is adequate, relevant, not excessive, and processed for limited purposes. We will never collect any unnecessary personal data from you and do not process your information in any way, other than as specified in this Notice.

You may share your personal data with us for a variety of reasons. We use different methods to collect data from and about you including through:

- Direct interactions. You may give us your identity and contact data by filling in forms or by corresponding with us by post, phone, email or otherwise.

In limited circumstances third parties may provide your personal data to us, such as nominated referees, official bodies (such as regulators or criminal record bureaus) and medical professionals.

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). We may collect, use, store and transfer different kinds of personal data about you which may include, but is not limited to:

Personal data collected in support of your employment includes (but is not limited to):

- identity data including, first name, unmarried name, last name, marital status, title, date of birth and gender;
- contact data including physical address, personal email address and telephone number;
- geographical location;
- details of your education, qualifications, skills, experience;
- employment records (including professional memberships, references, work history employment history, including start and end dates with previous employers and with Clancy);
- your photograph;
- the terms and conditions of your employment;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- bank account, national insurance number and other tax-related information;
- information on your marital status, next of kin, dependants, and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- Information on any criminal record;
- details of your working patterns, work location and attendance at work;
- details of holiday, sickness absence, family leave and sabbaticals, and other reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information on any medical or health conditions, including whether you have a disability for which we need to make reasonable adjustments;
- details of trade union membership;
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief;
- health and medical information in relation to any occupational health assessments, monitoring, or wellbeing programmes you participate in;
- other personal details included in a CV, application form or cover letter or that you otherwise voluntarily provide to us;
- CCTV footage and access control data (if attending our premises) (including gathering CCTV images from intruder movement-activated cameras;
- your vehicle's registration number (for our ANPR-operated car park barrier); and

- with regard to your use of any work telephones supplied by Clancy, description, duration, number of calls, destination of call, where the call is made from (e.g. mobile or fixed line), date and time of call, caller's location and call recipient's location.

Collection and use of special categories of personal data and criminal offence data

As stated above, in some of the processing described on this Notice we may collect special categories of personal data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data). We may also occasionally collect information about criminal convictions and offences (e.g. in relation to internal investigations we carry out).

We may collect and process the following special categories of personal data when you voluntarily provide them for the following legitimate business purposes, to carry out our obligations under employment law, for the performance of the employment contract, or as applicable law otherwise permits:

- fingerprint and facial information (biometric data) used to allow password-less sign-in to sites, and for attendance records, contract support and onboarding purposes;
- trade union membership information for the purpose of paying trade union premiums;
- physical or mental health information or disability status to comply with health and safety obligations in the workplace, to make appropriate workplace accommodations, as part of sickness absence monitoring, for occupational health assessments, monitoring or wellbeing programmes and to administer benefits; and
- race or ethnic origin, religious affiliation, health information and sexual orientation to ensure meaningful equal opportunity monitoring and reporting.

Where we have a legitimate need to process special categories of personal data for purposes not identified above, we will only do so only after providing you with notice and, if required by law, obtaining your prior, express consent.

How we use your personal data

We will only use your personal data when the law allows us to.

We will use your personal data in the following circumstances:

- sharing internally with Clancy employees and sub-contractors;
- staff administration (including payroll and benefits administration);
- maintaining accurate and up to date employment records and contact details (including emergency contacts), and maintaining records of your contractual and statutory rights;
- operating and keeping records of disciplinary and grievance processes, to ensure acceptable workplace conduct;
- assessing qualifications for a particular job or task;
- conducting our promotion processes;
- operating and keeping records of absence to ensure that you are receiving the pay or other benefits to which you are entitled;
- operating and keeping records of other types of leave (including maternity, paternity, adoption, parental and shares parental leave) to ensure: effective workforce management; so that we can comply with duties in relation to leave entitlement; and to ensure that you are receiving the correct pay or other benefits to which you are entitled;
- ensuring effective general HR and business administration;
- gathering evidence for disciplinary action or termination;

- conducting performance reviews and determining performance requirements;
- drug and alcohol testing, and the completion and storing of drug and alcohol forms;
- DVLA licence check for any Clancy staff member who drives a Clancy vehicle, or spouse or other permitted family member in relation to company cars;
- mailings for postal communications with staff, for example to provide information about mental health resources that staff can access; raising awareness of initiatives which are core to Clancy's values and capturing staff's ideas to improve the business; or news or information emails or SMS texts);
- ascertaining the relevant individuals for the annual Clancy Awards;
- processing of request forms for fuel payment cards;
- business management and planning;
- accounting and auditing;
- education, training, and development requirements;
- health administration services;
- complying with health and safety obligations;
- sending gestures of goodwill as appropriate at relevant times throughout the year;
- providing references on request for current or former staff members;
- responding to and defending against legal claims;
- occupational health assessments, monitoring or wellbeing programmes;
- maintaining and promoting equality in the workplace;
- provide to staff compliments and praise that were made by members of the public;
- manage training activity records on our Learning Management System;
- investigate Health, Safety and Environmental incidents, for example utility damage or personal injury claims;
- comply with Health and Safety legal compliance (for example, maintaining an accident book);
- investigate data protection related internal investigations and investigations of alleged noncompliance with data protection legislation;
- facilitate Clancy's compliance with data subject rights requests and other compliance duties, for example Data Subject Access Requests, personal data erasure requests, personal data rectification requests etc;
- manage internal investigations (in relation to the following types of investigations: alleged fraud by Clancy staff members, alleged H&S breaches, whistleblowing claims, internal disciplinary matters);
- investigate drivers' post-incident (e.g., collision) or complaint investigations to gather details to determine escalation outcome);
- investigate and resolve enquiries and complaints;
- prevent and detect crime;
- maintain Mileage and Car Drivers spreadsheets for MOT and tracker information purposes;
- use your fingerprint and facial information to allow for password-less access;
- allow entry into the Clancy Head Office (by virtue of the ANPR sensor-operated car park barrier); and
- supporting your use of work telephones supplied by us.

Our lawful bases for processing your personal data

Our lawful bases are:

- where we need to comply with a legal obligation;
- where we need to perform the employment contract we are about to enter into or have entered into with you;

- where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests;
- with your consent if applicable law requires consent.

We may process your personal data without your knowledge or consent where required by applicable law or regulation. Where we have relied on legitimate interests as the lawful basis for processing personal data, we have ensured that your privacy rights and freedoms are not overridden.

We may also process your personal data for our own legitimate interests, including for the following purposes:

- to prevent fraud; and
- to conduct data analytics analyses to review and better understand staff retention and attrition rates.

You will not be subject to decisions by Clancy based on automated data processing without your prior consent.

Who we share your personal data with externally

We will only disclose your personal data to third parties where required by law or to our employees, contractors, designated agents, or third-party service providers who require such information to assist us with administering the employment relationship with you, including third-party service providers who provide services to us or on our behalf.

Third-party service providers may include, but are not limited to, payroll processors, benefits administration providers, occupational health service providers and data storage or hosting providers. In the event that your role requires that we obtain pre-employment background checks from third parties, relevant personal data will be shared to support this process.

The recipient third parties are:

- our clients such as water and other utility companies;
- suppliers who provide services on behalf of Clancy, including Matrix Telematics; Zellis; Innovation LLP; Synlab; Eye Care Plus; SSS Management Services; Safer Scotland Ltd; IFS; Sign In; Knowbe4; Service Desk Plus; Manageengine; courier companies; Aptumo; Oneserve; Sphera Cloud; RPS Occupational Health Ltd; Learning Pool Ltd; OneAdvanced; Peoplebank; Virgin Media; Hudson Contract; Salary Finance Ltd; Vodafone; and Onecom Ltd (and its three UK-based sub-processors Mainline Digital Communications Limited; Plan.com; Tariffmatch Global Ltd, and one in India, Onecom Technology (India) Private Limited);
- other third parties who perform services on our behalf, including insurers, brokers pension providers and recruitment agencies; and professional advisors to Clancy, such as auditors and tax consultants;
- public bodies and regulatory authorities such as the Health & Safety Executive (including police and law enforcement agencies);
- providers of our IT and system administrative services; and
- any representative whom you have authorised to act on your behalf.

Data security

We take data protection seriously, and as such, we have internal policies/procedures (such as Data Protection Policy, Data Breach and Incident Management Policy, and Records Management Policy). We also maintain a range of security controls in place to ensure that your personal data is not lost, accidently destroyed, misused or disclosed, and is not accessed except by staff in the performance of their duties.

We have implemented appropriate physical, technical, and organizational security measures designed to secure your personal data against accidental loss and unauthorized access, use, alteration, or disclosure. In addition, we limit access to personal data to those employees, agents, contractors, and other third parties that have a legitimate business need for such access.

We maintain operational, technical and physical safeguards designed to protect personal information against accidental, unlawful or unauthorised destruction, loss, alteration, access, disclosure or use. We will store your personal data securely in a number of locations, including on Clancy sites and IT systems (including email and servers). The data of the server log files are stored separately from any personal data provided by users.

Personal data is retained in a range of locations, including your paper-based personnel files, in IFS and other IT systems (including the Clancy email system and network drive).

We take your privacy very seriously and will never sell your data.

International transfers of personal information

Onecom Ltd passes your personal data to its subsidiary in India, Onecom Technology (India) Private Limited. India does not have an adequacy decision from the UK Government. Such data transfers are therefore protected by the safeguard of being made under a contract between Onecom Ltd and Onecom Technology (India) Private Limited which contains the EU's most recent standard contractual clauses as amended by the ICO's UK Addendum. You can obtain a copy of the EU standard contractual clauses as amended by the UK Addendum by writing to our DPCO at the email address shown at the foot of this Notice.

Data retention

Except as otherwise permitted or required by applicable law or regulation, we will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, as required to satisfy any legal, accounting, or reporting obligations, or as necessary to resolve disputes. If you fail a drug or alcohol test, your test results data may be retained indefinitely, so that we may avoid reemployment.

To determine the appropriate retention period for personal data, we consider applicable legal requirements, the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes we process your personal data for, and whether we can achieve those purposes through other means.

Under some circumstances we may anonymize your personal data so that it can no longer be associated with you. We reserve the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to you or your consent. Once you are no longer an staff member of Clancy we will retain and securely destroy your personal data in accordance with our document retention policy and applicable laws and regulations.

Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data.

You have the right to:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request rectification of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

- if you want us to establish the data's accuracy;
- where our use of the data is unlawful, but you do not want us to erase it;
- where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; and or
- you have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request the transfer of your personal data to you or to a third party (data portability). We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

If you wish to exercise any of the rights set out above, please contact the Head of Internal Investigations (DPCO) at Roland.Thomas@theclancygroup.co.uk

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

If you wish to exercise your rights and it relates to personal information you provided to another organisation that contracted with Clancy for Clancy to provide services to you then you must exercise your rights directly with that organisation.

What we may need from you

We may request specific information from you to help us confirm your identity and your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

Changes to this Notice and your duty to inform us of changes

We reserve the right to update this Notice at any time, and we will provide you with a new Notice when we make any updates. If we would like to use your previously collected personal data for different purposes than those we notified you about at the time of collection, we will provide you with notice and, where required by law, seek your consent before using your personal data for a new or unrelated purpose. We may process your personal data without your knowledge or consent where required by applicable law or regulation.

We keep this Notice under regular review. It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

Contact details

If you have any questions about this Notice or how we handle your personal data, or would like to request access to your personal data, please contact our DPCO:

Roland Thomas at: roland.thomas@theclancygroup.co.uk

If you are unsatisfied with our response to any issues that you raise with us, you may have the right to make a complaint with to the Information Commissioner's Office:
Information Commissioner's Office
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Helpline Number: 0303 123 1113