GDPR Data Privacy Policy

Policy Number	15
Version	5
Policy Contact	Matthew Betteridge
Date Issued	18th May 2018
Reviewed	06th May 2026
Next Review Date	06th May 2027
Target Audience	Staff, Consultants and Agency Workers
Approved by	OneCall24 Policy Team

1 Overview – Legislative References

This Document defines OneCall24's Data Privacy Policy and is to be used in conjunction with OneCall24's Data Retention Policy to adhere to the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and relevant amendments introduced by the Data (Use and Access) Act 2025.

The Privacy Policy consists of the following sections:

1. Overview;
2. Data Protection Principles;
3. How we define personal data;
4. How we define special categories of personal data;
5. How we define processing;
6. How will we process your personal data;
7. Examples of when we might process your personal data;
8. Sharing your personal data;
9. How should you process personal data for the business?
10. How to deal with data breaches;
11. Data Protection Impact Assessments (DPIAs)
12. Subject access requests;
13. Your data subject rights;
14. Training and Awareness

and the following Detailed Policies

15. Email Acceptable Usage Policy.
16. Internet Acceptable Usage Policy.
17. Social Media Acceptable Use Policy.
18. Corporate Infrastructure Policy.
19. Business Application Policy.
20. Infrastructure Monitoring Policy.

2 Overview

One Call 24 Limited (company registration number 09732799) of 239 Old Marylebone Road, London NW1 5QT ("OneCall24") takes the security and privacy of personal data seriously. We collect and use personal data as part of the operation of our business and to manage our relationships with staff, consultants and agency workers. We are committed to complying with our legal obligations under the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018, and subsequent amendments, and any applicable amendments to UK data protection legislation from time to time. This policy is intended to fulfil our transparency obligations under Articles 13 and 14 of the UK GDPR.

2.1 This policy applies to all staff, consultants and Agency Workers of OneCall24. You should read this policy alongside your contract of employment (or contract for services, as applicable) and any other privacy notices or policies we issue from time to time in relation to your personal data.

2.2 OneCall24 has appropriate technical and organisational measures in place to protect the security of personal data and to ensure it is retained for no longer than is necessary for the purposes for which it was collected. These measures include physical, technical and administrative safeguards. Personal data is retained in accordance with applicable legal and regulatory requirements and OneCall24's Data Retention Policy, which sets out retention periods by data category and is reviewed regularly. Our approach is informed by recognised best-practice guidance, including guidance issued by the CIPD where relevant.

2.3 For the purposes of the UK GDPR, OneCall24 is the **data controller** in respect of personal data processed under this policy. This means that we determine the purposes for which, and the manner in which, personal data is processed.

2.4 This policy explains how OneCall24 collects, holds and processes personal data, the lawful bases on which processing is carried out, and the rights of individuals as data subjects. It also sets out the responsibilities and obligations of all persons working for, or on behalf of, OneCall24 when obtaining, handling, processing or storing personal data in the course of their duties.

2.5 OneCall24 has appointed a Head of Compliance with responsibility for overseeing data protection compliance and acting as the primary point of contact for data protection matters. OneCall24 is not legally required to appoint a statutory Data Protection Officer under Article 37 of the UK GDPR; however, we ensure that data protection responsibilities are managed at a senior level in accordance with the accountability principle.

This policy does not form part of any contract of employment or contract for services and may be amended by OneCall24 at any time. Where there is any conflict between this policy and applicable data protection legislation, the legislation shall prevail.

3 Data Protection Principles

Personal data must be processed in accordance with the data protection principles set out in Article 5 of the UK GDPR. Accordingly, personal data must:

- be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');
- be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');
- be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ('data minimisation');
- be accurate and, where necessary, kept up to date, with every reasonable step taken to ensure that inaccurate personal data is erased or rectified without delay ('accuracy');
- be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed ('storage limitation');
- be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'); and
- be subject to the accountability principle, meaning that OneCall24 is responsible for, and must be able to demonstrate, compliance with all of the above principles ('accountability').

4 How we define personal data

4.1 '**Personal data**' means any information relating to an identified or identifiable living individual (a '**data subject**'). An identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual. Personal data includes expressions of opinion about an individual and indications of intentions in respect of that individual. It does not include data which has been anonymised so that individuals are no longer identifiable.

4.2 This policy applies to all personal data processed by OneCall24, whether the data is stored electronically, on paper, or in any other format or medium.

4.3 Personal data may be provided directly by you, obtained from third parties (such as former employers, referees, medical professionals, regulatory bodies or credit reference agencies), or generated by OneCall24 in the course of its business activities. Personal data may be collected or created during the recruitment process, throughout the duration of an individual's employment or engagement, and following the termination of that employment or engagement. Personal data may also be created by managers, colleagues or systems operated by OneCall24.

4.4 Depending on the nature of your role and your relationship with OneCall24, we may collect and use the following categories of personal data:

- Personal identification and contact details, including name, title, home address, email address and telephone numbers;
- Date of birth;
- Gender;
- Marital status and dependants or family details;
- Next of kin and emergency contact details;
- National Insurance number;
- Bank account details, payroll records and tax status information;

- Salary, remuneration, pension and benefits information;
- Annual leave and absence records;
- Start date and end date of employment or engagement;
- Contractual information relating to employment or services;
- Work location or place of employment;
- Copies of driving licences or other identification documentation where required;
- Recruitment and right-to-work information, including application forms, CVs, references, qualifications, professional memberships and pre-employment assessments;
- Employment and engagement records, including job title, work history, working hours, training records and continuing professional development;
- Compensation history;
- Performance management and appraisal information;
- Information relating to conduct, disciplinary and grievance matters, including investigations and outcomes (whether or not you are the primary subject);
- Training and mandatory compliance records;
- CCTV footage, swipe-card access records and other electronic monitoring data;
- Information relating to the use of OneCall24's IT, communication, telephone and security systems;
- Images, photographs or video recordings where applicable; and
- Any other personal data which OneCall24 may notify you of from time to time in accordance with the law.

5 How we define special categories of personal data

5.1 '**Special categories of personal data**' are types of personal data revealing or relating to:

- racial or ethnic origin;
- religious or philosophical beliefs;
- sexual orientation;
- political opinions;
- trade union membership;
- physical or mental health, including medical conditions, sickness and health records;
- genetic data; and
- biometric data, where used for the purpose of uniquely identifying an individual.
- We may hold and use any of these special categories of your personal data in accordance with the law.

5.2 Information relating to criminal convictions and offences is not treated as special category data but is subject to separate protections under Article 10 of the UK GDPR and the Data Protection Act 2018. Such data will only be processed where permitted by law and subject to appropriate safeguards.

OneCall24 will only collect and process special categories of personal data or criminal convictions data where there is a lawful basis for doing so and, where required, an additional statutory condition is met.

6 How we define processing

6.1 **'Processing'** means any operation or set of operations which is performed on personal data, whether or not by automated means, including but not limited to:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- Retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes the processing of personal data that forms part of a filing system, as well as fully or partly automated processing.

7 How will we process your personal data?

OneCall24 will process your personal data, including special categories of personal data, in accordance with our obligations under the UK GDPR and other applicable legislations.

7.1 We will process personal data for one or more of the following lawful basis:

- where processing is necessary for the performance of a contract of employment or a contract for services to which you are a party;
- where processing is necessary for compliance with a legal obligation to which OneCall24 is subject; and
- where processing is necessary for the purposes of OneCall24's legitimate interests, or the legitimate interests of a third party, provided that such interests are not overridden by your rights and freedoms.

7.2 In most circumstances, OneCall24 does not rely on consent as a lawful basis for processing personal data in an employment or engagement context, due to the imbalance of power between the organisation and the individual. Where consent is relied upon, it will be explicit, documented, limited to a specific purpose and capable of being withdrawn at any time without detriment.

7.3 We will not process personal data for purposes that are incompatible with those for which it was originally collected without first providing you with appropriate information and identifying a lawful basis for the new processing.

7.4 If you choose not to provide certain personal data, OneCall24 may be unable to fulfil some contractual, statutory or operational obligations. For example, without bank account details we may be unable to pay salary, and without certain health information we may be unable to comply with health and safety or reasonable adjustment obligations. The consequences of non-provision will be explained at the point data is collected where relevant.

7.5 Where OneCall24 relies on consent as a lawful basis or condition for processing personal data or special categories of personal data, such consent will be explicit, specific and documented. In such cases, consent may be withdrawn at any time by contacting the Head of Compliance (gdpr@onecall24.co.uk), without detriment.

In most employment and engagement contexts, OneCall24 does not rely on consent due to the imbalance of power between the organisation and the individual.

8 Examples of when we might process your personal data

8.1 OneCall24 processes personal data at various stages of the recruitment, employment or engagement lifecycle and, where necessary, following the termination of employment or engagement.

8.2 By way of example, we may process personal data for the following purposes:

- to assess suitability for recruitment or engagement;
- to determine remuneration, benefits and other contractual terms;
- to administer and manage the employment or engagement relationship;
- to verify identity and legal entitlement to work in the United Kingdom;
- to perform, manage and, where applicable, terminate contracts of employment or services;
- to provide training, development and performance review;
- to assess qualifications, competence and suitability for specific roles, responsibilities or promotion;
- to manage performance, conduct, attendance and absence;
- to make decisions relating to continuation, change or cessation of employment or engagement;
- to investigate, manage and resolve disciplinary, capability, grievance or whistleblowing matters;
- to determine and implement reasonable adjustments to roles or workplaces where required;
- to monitor equality, diversity and inclusion in compliance with applicable legislation;
- to monitor and protect the security of OneCall24's premises, systems, networks, staff, customers and other individuals;
- to monitor and manage health and safety risks affecting staff, contractors, customers and third parties;
- to administer payroll, taxation, pension schemes and contractual benefits and to liaise with benefit or pension providers;
- to comply with obligations relating to tax, National Insurance and statutory reporting;
- to provide references where requested and permitted by law;
- to monitor use of IT, communication and security systems in accordance with OneCall24 policies;
- to ensure network and information security, including the prevention of unauthorised access or malicious activity;
- to monitor compliance with internal policies, procedures and contractual obligations;
- to comply with employment, immigration, health and safety, equality, tax and other applicable legal or regulatory requirements;
- to conduct business analysis, including workforce planning, retention and attrition analysis;
- to respond to insurers or advisers in connection with insurance arrangements relating to individuals;
- to manage, plan and operate the business, including accounting, audit and risk management activities;
- to prevent, detect or investigate fraud, misconduct or criminal activity;
- to establish, exercise or defend legal claims and to comply with court, tribunal or regulatory orders; and
- for other compatible purposes which are lawful and which are notified to individuals as required by the UK GDPR.

8.3 OneCall24 will only process special categories of personal data where permitted by law and where an appropriate lawful basis and statutory condition under Article 9 of the UK GDPR and the Data Protection

Act 2018 applies. Such processing will be limited to what is necessary and subject to appropriate safeguards.

8.4 In most cases, OneCall24 does not rely on consent as a condition for processing special categories of personal data in an employment or engagement context. Instead, such data may be processed where, for example:

- processing is necessary for performing rights or obligations under employment, social security or social protection law;
- processing is necessary to protect the vital interests of the data subject or another individual where consent cannot be given;
- the data has been manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims; or
- processing is necessary for occupational health, medical diagnosis, assessment of working capacity or management of health or social care systems, subject to confidentiality safeguards.

Where consent is required by law, it will be explicit, specific and capable of being withdrawn at any time without detriment.

8.5 Special categories of personal data may be processed in particular for the following purposes, where lawful and necessary:

- information relating to race, ethnic origin, religion, sexual orientation or gender for equality, diversity and inclusion monitoring;
- information relating to sickness absence, family-related leave or other statutory leave to comply with employment and related legislation; and
- health and medical information to manage absence, assess fitness for work, provide statutory or contractual benefits, make reasonable adjustments, and ensure health and safety obligations are met.

8.6 6 OneCall24 does not carry out automated decision-making, including profiling, which produces legal effects concerning individuals or similarly significantly affects them within the meaning of Article 22 of the UK GDPR.

9 Sharing your personal data

9.1 OneCall24 may share personal data with third parties where necessary and lawful to do so, including where required to fulfil contractual obligations, comply with legal requirements, or pursue our legitimate interests. Such third parties may include, where appropriate:

- pension scheme administrators and benefit providers;
- payroll providers and professional advisers;
- IT software, hardware and systems providers;
- security, CCTV and alarm service providers;
- medical professionals and occupational health providers;
- regulatory bodies and professional organisations;
- insurers;
- group companies, contractors, agents, suppliers and service providers acting on our behalf.

9.2 Where third parties process personal data on our behalf as data processors, OneCall24 ensures that appropriate written contracts are in place requiring them to:

- process personal data only on documented instructions from OneCall24;
- maintain appropriate confidentiality and security measures;
- comply with applicable data protection legislation; and
- assist OneCall24 in meeting its obligations under the UK GDPR.

9.3 Third parties may process personal data for purposes such as administering payroll, pensions and benefits, providing IT systems or services, delivering professional or outsourced services, or assisting OneCall24 in meeting its contractual or legal obligations. Personal data will not be shared with third parties for their own independent purposes unless permitted or required by law.

9.4 In some circumstances, personal data may be transferred to, stored in, or accessed from countries outside the United Kingdom. Where this occurs, OneCall24 will ensure that appropriate safeguards are in place to protect personal data in accordance with the UK GDPR. Such safeguards may include, where applicable:

- transfers to countries recognised by the UK government as providing an adequate level of data protection;
- the use of the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses; and
- the completion of transfer risk assessments and implementation of supplementary measures where required.

Further information about international transfers may be obtained from the Head of Compliance upon request.

10 How should you process personal data for the business?

10.1 All individuals who work for, or on behalf of, OneCall24 share responsibility for ensuring that personal data is collected, used, stored and handled in accordance with this policy and applicable data protection legislation.

10.2 The Head of Compliance is responsible for overseeing this policy and data protection compliance within OneCall24. Any questions or concerns relating to data protection or this policy should be directed to the Head of Compliance.

10.3 All personnel must comply with the detailed policies that accompany this policy and govern the use of OneCall24 systems and infrastructure, including:

- Email Acceptable Usage Policy.
- Internet Acceptable Usage Policy.
- Social Media Acceptable Use Policy.
- Corporate Infrastructure Policy.
- Business Application Policy.
- Infrastructure Monitoring Policy.

10.4 You must only access personal data where necessary for the performance of your role and where you are authorised to do so. Personal data must only be used for the specific lawful purpose for which it was obtained.

10.5 Personal data must not be shared informally or disclosed to unauthorised individuals.

10.6 You must take appropriate steps to keep personal data secure and protect it from unauthorised access, loss or disclosure.

10.7 You should ensure that personal data you process is accurate and kept up to date, and notify OneCall24 promptly of any changes to your own personal details.

10.8 You should avoid making unnecessary copies of personal data and must ensure that any copies are stored securely and disposed of appropriately.

10.9 Strong passwords must be used in accordance with OneCall24's security policies and must not be shared.

10.10 Computer screens must be locked or devices logged out when left unattended.

10.11 Where possible and appropriate, personal data should be anonymised or pseudonymised so that individuals cannot be readily identified.

10.12 Personal data must not be saved to personal devices or non-approved systems unless expressly authorised.

10.13 Personal data must not be transferred outside the United Kingdom except where such transfer complies with applicable data protection law and has been authorised in accordance with OneCall24 procedures.

10.14 Paper records containing personal data must be stored securely, for example in locked drawers or cabinets, and must not be left unattended.

10.15 Personal data must not be removed from OneCall24 premises or systems without appropriate authorisation.

10.16 When no longer required, personal data must be disposed of securely, including through shredding or secure electronic deletion, in accordance with OneCall24's Data Retention Policy.

10.17 You should seek guidance from the Head of Compliance if you are unsure about data protection requirements or identify any potential improvements to data protection or security practices.

10.18 Failure to comply with this policy may result in disciplinary action in accordance with OneCall24's disciplinary procedures. Serious breaches may be treated as gross misconduct and could result in dismissal.

10.19 It is a criminal offence under data protection legislation to deliberately conceal, destroy or alter personal data that is subject to a valid subject access request. Such conduct will be treated as gross misconduct.

10.20 OneCall24 maintains a Record of Processing Activities in accordance with Article 30 of the UK GDPR, documenting the categories of personal data processed, the purposes of processing, lawful bases, recipients, retention periods and applicable safeguards. The Record of Processing Activities is maintained by the Head of Compliance and is reviewed and updated as necessary.

11 How to deal with data breaches

11.1 OneCall24 has appropriate technical and organisational measures in place to reduce the likelihood of personal data breaches. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

If a personal data breach occurs (whether relating to staff, contractors or any other individuals), OneCall24 will promptly assess the incident, record relevant details, and maintain appropriate documentation to meet its accountability obligations under the UK GDPR.

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, OneCall24 will notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Where required by law, affected individuals will also be notified without undue delay.

11.2 If you become aware of, or suspect, a personal data breach, you must immediately notify the Head of Compliance and preserve any relevant evidence. Further detail on incident management, escalation and notification is set out in the GDPR Data Breach Policy, available from the Head of Compliance.

12 Data Protection Impact Assessments (DPIAs)

OneCall24 recognises its obligation under the UK GDPR to carry out Data Protection Impact Assessments (DPIAs) where processing is likely to result in a high risk to the rights and freedoms of individuals. DPIAs help identify, assess and mitigate data protection risks at an early stage.

12.1 A DPIA will be conducted in particular where processing involves:

- the introduction of new technologies or systems that involve personal data;
- the large-scale processing of special categories of personal data or criminal convictions data;
- systematic monitoring of individuals, including through CCTV or other surveillance technologies; or
- profiling or automated decision-making that produces legal effects or similarly significant impacts on individuals.

The DPIA will be led by the Head of Compliance and will include:

- A description of the processing and its purposes.
- An assessment of the necessity and proportionality of the processing.
- An evaluation of the risks to the rights and freedoms of individuals; and
- The measures envisaged to address and mitigate those risks and demonstrate compliance.

12.2 All staff and contractors must consult the Head of Compliance before initiating any new project, system or process that may require a DPIA.

13 Subject access requests

13.1 Individuals have the right to make a **subject access request ("SAR")** to obtain confirmation of whether OneCall24 processes their personal data and, where applicable, to access that data. Requests do not need to refer to the UK GDPR or use specific wording to be valid.

If you receive a SAR or believe a request may constitute a SAR, you must forward it immediately to the Head of Compliance.

13.2 SARs should be addressed to the Head of Compliance at gdpr@onecall24.co.uk. OneCall24 will respond without undue delay and in any event within one month of receipt. This period may be extended by up to two additional months where requests are complex or numerous, in which case the individual will be informed.

13.3 There is no fee for making a SAR. However, where a request is manifestly unfounded or excessive, OneCall24 may charge a reasonable administrative fee or refuse to act on the request in accordance with the UK GDPR. Further detail is contained in the GDPR Subject Access Request Policy, available from the Head of Compliance.

14 Your data subject rights

14.1 You have the right to be informed about how OneCall24 processes your personal data, including the purposes of processing and the lawful bases relied upon, as set out in this policy and related privacy information.

14.2 You have the right to access your personal data by making a subject access request.

14.3 You have the right to request the rectification of inaccurate or incomplete personal data.

14.4 You have the right to request the erasure of your personal data where OneCall24 is no longer entitled to process it or where it is no longer necessary for the purpose for which it was collected, subject to applicable legal exemptions.

14.5 You have the right to request restriction of processing while the accuracy or lawfulness of processing is contested.

14.6 You have the right to object to processing where OneCall24 relies on legitimate interests as the lawful basis and where you believe that your rights and interests override those interests. You also have the right to object at any time to processing for direct marketing purposes.

14.7 You have the right to data portability in respect of personal data you have provided to OneCall24 and which is processed on the basis of consent or contract, where this is technically feasible.

14.8 You have the right not to be subject to automated decision-making, including profiling, where such decision-making produces legal effects concerning you or similarly significantly affects you, except where permitted by law.

14.9 You have the right to be notified of a personal data breach where the breach is likely to result in a high risk to your rights and freedoms.

14.10 In most employment and engagement contexts, OneCall24 does not rely on consent as a lawful basis for processing personal data. Where consent is relied upon, you have the right to refuse consent or to withdraw consent at any time without detriment.

14.11 **To exercise any of your data protection rights**, including making a subject access request or exercising the rights set out above, you should contact the Head of Compliance at **gdpr@onecall24.co.uk**. Requests will be handled in accordance with the UK GDPR and applicable statutory time limits.

14.12 You have the right to lodge a complaint with the Information Commissioner's Office if you believe that your personal data has been processed unlawfully. Further information, including contact details, is available at **www.ico.org.uk**.

15 Training and Awareness

All staff, consultants and agency workers at OneCall24 are required to complete mandatory data protection training as part of their induction and at regular intervals thereafter. This training ensures that individuals

understand their responsibilities under this policy, the UK General Data Protection Regulation, and other applicable data protection legislation.

Refresher training is provided at least annually and additional training is delivered where there are material changes to legislation, regulatory guidance, internal policies, systems or procedures, or where specific data protection risks are identified. Attendance and completion of training is monitored, recorded and evidenced by the HR department as part of OneCall24's accountability obligations.

Failure to complete mandatory data protection training may result in remedial action being taken and, where appropriate, may be addressed through OneCall24's performance or disciplinary procedures.

DETAILED POLICIES

16 Email Acceptable Usage Policy.

16.1 Email must be treated as a formal business communication tool. All emails sent or received using OneCall24 systems must be professional, accurate and appropriate. You should be aware that emails can be forwarded, disclosed or retrieved and may form part of legal or regulatory proceedings.

16.2 Care must be taken when referring to individuals, including colleagues, customers or third-party contacts, as they have rights to privacy and data protection. If you are unsure whether it is appropriate to include identifying information, you should seek guidance from your line manager or the Head of Compliance.

16.3 Documents or files containing personal data, confidential information or commercially sensitive information must not be attached to emails unless they are protected using approved encryption or security measures provided by OneCall24.

16.4 Emails must not contain language or material that is offensive, abusive, discriminatory or otherwise inappropriate. All email communications must comply with OneCall24's Equality, Diversity and Anti-Harassment policies. Remarks or jokes may constitute harassment regardless of intent.

16.5 Personal, derogatory or defamatory comments must not be made in email communications.

16.6 You must not access, interfere with or impersonate another person's email account, or send emails that appear to originate from another individual without authorisation.

16.7 Emails must not be forwarded to third parties for non-business purposes without appropriate authority.

16.8 Email communications should be clear, concise and business-focused. You should avoid copying individuals unnecessarily.

17 Internet Acceptable Usage Policy.

The following is guidance on the acceptable use of Internet according to Industry best practices at the time of publication:

- Internet searches and activity should be strictly business related.
- Searches must not contain any swear words or phrases which could be considered offensive.
- All internet activity should comply with OneCal24l's equal opportunities policy/anti-harassment policy. Remarks or jokes sent by internet channels can amount to harassment and, as with all harassment complaints, the intention of the party sending the e-mail is not relevant Internet based comments could well form the foundation of a discrimination claim when they contain

remarks or jokes related to race, sex, sexual orientation, disability, age or religion/belief which one of the recipients finds offensive.
- Do not tamper with or use anyone else's network account for internet usage.
- For more information on Social Media, please see the Social Media Acceptable Use Policy.

Subject to the balance of this policy, employees may use the Internet access provided by OneCall24 for:

- Work-related purposes.
- Sending and receiving personal email messages, provided that if email messages are sent with a OneCall24 email address in the From: or Reply-To: header, a disclaimer shall accompany the email to the effect that the views of the sender may not represent those of OneCall24.
- Reading and posting personal Usenet messages on the same condition specified above.
- Using instant messaging software for personal purposes.
- Accessing the World Wide Web for personal purposes.
- Utilising any other Internet service or protocol for personal purposes after obtaining permission to do so from OneCall24.

Provided in each case that the personal use is moderate in time, does not incur significant cost for OneCall24 and does not interfere with the employment duties of the employee or his or her colleagues.

Except during an employee's duties or with the express permission of OneCall24 the Internet access provided by OneCall24 may not be used for:

- personal commercial purposes;
- sending unsolicited bulk email;
- disseminating confidential information of OneCall24;
- disseminating the names, addresses and other personal data of OneCall24 employees or the employees of other companies with which OneCall24 does business or has contact;
- any illegal purpose;
- knowingly causing interference with or disruption to any network, information service, equipment or any user thereof;
- disseminating personal contact information of officers or employees of OneCall24 without their consent; and
- causing any other person to view content which could render OneCall24 liable pursuant to equal opportunity, equality or sex discrimination legislation at the suit of that person; or downloading or requesting software or media files or data streams that the employee has reason to believe will use a greater amount of network bandwidth than is appropriate.

Responsibility for use of the Internet that does not comply with this policy lies with the employee so using it, and such employee must indemnify OneCall24 for any direct loss and reasonably foreseeable losses suffered by OneCall24 by reason of the breach of policy. This may have a significant legal and financial impact on the employee and their family.

OneCall24 will review any alleged breach of this Acceptable Use Policy on an individual basis. If the alleged breach is of a very serious nature which breaches the employee's duty of fidelity to OneCall24 (for example, emailing confidential information of OneCall24 to a competitor), the employee shall be given an opportunity to be heard in relation to the alleged breach and if it is admitted or clearly established to the satisfaction of OneCall24 the breach may be treated as grounds for dismissal.

18 Social Media Acceptable Use Policy.

Any communications that employees **make in a professional capacity** through social media must not:

- make defamatory comments about individuals or other organisations or groups;
- give away confidential information about an individual (such as a colleague or partner contact) or organisation (such as a partner institution) without lawful basis;
- breach confidentiality (for example, by revealing confidential intellectual property or information owned by OneCall24);
- discuss OneCall24's internal workings (such as agreements it is reaching with customers or partners, or future business plans that have not been communicated publicly);
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual (for example by making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age).
- use social media to bully another individual (Including employees of OneCall24);
- post images or links to content that could be considered inappropriate, discriminatory or offensive;
- bring OneCall24 into disrepute (for example by criticising or arguing with customers, colleagues, partners or competitors);
- breach copyright (for example by using someone else's images or written content without permission);
- breach data protection or privacy legislation (for example by naming individuals or sharing personal data without a lawful basis); and
- fail to give acknowledgement where permission has been given to reproduce something.

Any communications that employees make **in a personal capacity** through social media must not:

- make defamatory comments about individuals or other organisations or groups.
- breach confidentiality (for example by: revealing confidential intellectual property or information owned by OneCall24);
- give away confidential information about an individual (such as a colleague or partner contact) or organisation (such as a partner institution);
- discuss OneCall24's internal workings (where such information has not been made publicly available)
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual (for example by making offensive or derogatory comments relating to protected characteristics);
- use social media to bully another individual (such as an employee of OneCall24);
- Post images or links to content that could be considered inappropriate, discriminatory or offensive;
- bring OneCall24 into disrepute (for example by criticising or arguing with customers, colleagues, partners or competitors);
- breach copyright (for example by using someone else's images or written content without permission);
- breach data protection or privacy legislation by sharing personal data without authorisation or a lawful basis; and
- fail to give acknowledgement where permission has been given to reproduce something.

19 Corporate Infrastructure Policy.

Corporate Infrastructure refers to all hardware, software, networks and information technology procured and controlled by OneCall24.

You are responsible for the security of data, accounts, and systems under your control:

- You must maintain system-level and user-level passwords in accordance with the following Password Policy:
  - Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends.
  - All PCs, PDAs, Smartphones, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
  - Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.
- You must ensure through legal or technical means that OneCall24 proprietary information, and personal data for which OneCall24 is responsible, is protected against unauthorised access, loss or disclosure and remains within OneCall24's control.
- You are responsible for ensuring the protection of assigned OneCall24 assets:
  - Laptops left at OneCall24 overnight must be properly secured or placed in a locked drawer or cabinet.
  - Promptly report any theft or loss of devices or data to one of OneCall24's Directors or your immediate line manager.
- Devices that connect to the OneCall24 network must comply with the following Minimum Access Policy:
  - OneCall24 business that results in the storage of proprietary information on personal or non-OneCall24 controlled environments, including devices maintained by a third party with whom OneCall24 does not have a contractual agreement, is prohibited unless expressly authorised. This specifically prohibits the use of an e-mail account that is not provided by, OneCall24 or its customer and partners, for company business.
  - Employees personal devices must only be used on wireless networks specifically provided by OneCall24 for personal usage. They must not be connected to any of OneCall24's business networks or used for any OneCall24 business activity without the prior written consent of at least one of OneCall24's Directors.
- Do not interfere with corporate device management or security system software, including, but not limited to antivirus, device management or security software products and tools maintained by OneCall24.

You are responsible for the security and appropriate use of OneCall24 network resources under your control. Using OneCall24 resources for the following is strictly prohibited:

- Causing a security breach to either OneCall24 or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.
- Causing a disruption of service to either OneCall24 or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

- Taking or assisting the taking of company records that contains the names, addresses and other details of persons (even if they are employees of OneCall24 or another company) outside OneCall24 network resources.
- Introducing honeypots, honeynets, or similar technology on the OneCall24 network.
- Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software. See the OneCall24 for additional information on copyright restrictions.
- Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Use of the Internet or OneCall24 network that violates the any of OneCall24 policies, or local laws.
- Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.
- Port scanning or security scanning on a production network unless authorized in advance by Information Security.

20 Business Application Policy.

The following Business Applications are approved for use on Corporate Infrastructure and BYOD devices used for business purposes:

1. Microsoft Outlook
2. Microsoft 365 applications (including Word, Excel, PowerPoint and OneDrive)
3. Microsoft Visio
4. Microsoft Project
5. Microsoft Teams
6. Google Chrome
7. Approved CRM systems
8. WhatsApp (business use only and subject to data protection controls)
9. Jobscience
10. Merit

Business Applications not on this list must not be used for business purposes under any circumstances. Transfer of data from approved Business Applications to non-approved Business Applications is strictly prohibited and will be considered misconduct.

The following is a non-exhaustive list of non-approved Business Applications:

1. Facebook
2. Twitter
3. Cloud Services
4. Bring Your Own Device (BYOD) SMS

21 Infrastructure Monitoring Policy.

OneCall24 recognise the employee's right to privacy and our responsibilities under law. In particular:

- We recognise that employees have a right to privacy in respect of their personal communications.
- We reserve the right to monitor employees' use of e-mail and the Internet to ensure compliance with OneCall24's Email Usage, Internet Usage and Social Media Acceptable Use

policies and to investigate any specific breaches of the policy where there is sufficient reason to do so.

Prior to monitoring, OneCall24 will carry out an impact assessment to assess the necessary extent of any monitoring, the nature of any adverse effect upon the employee and the safeguards required to an employee e.g. prior warning.

Monitoring will be conducted with the authorisation of a line manager on prior notice to the employee concerned. Monitoring may include any of the following:

- Reviewing Internet sites accessed.
- Reviewing time spent on e-mail and internet.
- Reviewing e-mails sent and received.
- Reviewing files attached to e-mails.
- Reviewing Uploads.
- Reviewing Downloads.
- Reviewing non-business behaviours.

This list is not exhaustive, and we reserve the right to use other techniques. Covert monitoring (i.e. where no warning is given) shall only be used where it is:

- Required by regulatory/legal obligations.
- Necessary to prevent or detect crime.
- Required to protect OneCall24's IT systems from damage (e.g. viruses).
- Gross misconduct is suspected.

The information will be collated by the individual monitoring and shared with the employee as soon as practical – this may be as part of an investigation conducted under OneCall24's disciplinary process.

OneCall24 keeps and may monitor logs of Internet usage which may reveal information such as which Internet servers (including World Wide Web sites) have been accessed by employees, and the email addresses of those with whom they have communicated.

OneCall24 may engage in real-time surveillance of Internet usage, monitor the content of email messages sent or received by its employees unless a copy of such message is sent or forwarded to OneCall24 by its recipient or sender in the ordinary way, and will not disclose any of the logged, or otherwise collected, information to a third party except under compulsion of law.