GDPR and Data Privacy Policy

Policy Number	15
Version	4
Policy Contact	Matthew Betteridge
Date Issued	18th May 2018
Reviewed	15th May 2024
Next Review Date	15th May 2025
Target Audience	Staff and Consultants
Approved by	OneCall24 Policy Team

Contents

1. GDPR Data Privacy Policy for Staff and Consultants

This Document defines OneCall24's Data Privacy Policy for Staff and Consultants ("Privacy Policy") and is to be used in conjunction with OneCall24's Data Retention Policy to adhere to the UK GDPR and Data Protection Act of 2018.

1.1. Overview

One Call 24 Limited (co. reg. no. 09732799 of 239 Old Marylebone Road, London NW1 5QT ("OneCall24") takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the UK GDPR and Data Protection Act of 2018 in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

This policy applies to all staff and consultants of OneCall24. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

OneCall24 has measures in place to protect the security of your data and retain it for no longer than is necessary. Our security systems include physical as well as computer security measures. Your data is held for no longer than the law requires, and we follow CIPD guidelines on retention guidelines for employment personal data. We will only hold data for as long as necessary for the purposes for which we collected it.

OneCall24 is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

This policy explains how we will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, OneCall24.

This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by us at any time. It is intended that this policy is fully compliant with the UK GDPR and Data Protection Act of 2018. If any conflict arises between those laws and this policy, we intend to comply with the UK GDPR and Data Protection Act of 2018.

1.2. Data Protection Principles

Personal data must be processed in accordance with seven '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently ('lawfulness, fairness and transparency');
- be collected and processed only for specified, explicit and legitimate purposes ('purpose limitation');
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed ('data minimisation');

- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay ('accuracy');
- not be kept for longer than is necessary for the purposes for which it is processed ('storage limitation');
- be processed securely ('integrity and confidentiality') and;
- As we are accountable for these principles and must be able to show that we are compliant ('accountability').

1.3. How we define personal data

'**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

We will collect and use the following types of personal data about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants/family details.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date and end date of employment.
- Information about your contract of employment.
- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references, qualifications and membership of any professional bodies and details of any pre-employment assessments and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history.
- Information relating to your performance and behaviour at work.

- Information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings).
- Disciplinary and grievance information.
- Training and CPD records.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information, telephone, alarm and communications systems.
- Your images, whether in CCTV, by photograph or video.
- Any other category of personal data which we may notify you of from time to time.

1.4. How we define special categories of personal data

'**Special categories of personal data**' are types of personal data consisting of information as to information about:

- your race or ethnicity, religious or philosophical beliefs, sexual orientation and political opinions;
- trade union membership;
- your health, including any medical condition, health and sickness records;
- genetic information and biometric data; and
- criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

1.5. How we define processing

'Processing' means any operation which is performed on personal data such as:

- 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 processing personal data which forms part of a filing system and any automated processing.

1.6. 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.

We will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or

- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 12 below.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

1.7. Examples of when we might process your personal data

We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

For example (and see section 7.5 below for the meaning of the asterisks):

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to administer the terms of your contract with us;
- to check you have the legal right to work for us/to work in the UK;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance*;
- to assess qualifications for a particular job or task, including decisions on whether to promote you;
- to decide whether and how to manage your performance, absence or conduct*;
- to make decisions about your continued employment or engagement;
- to make arrangements for the termination of our working relationship;
- to gather evidence for or carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;
- to monitor diversity and equal opportunities*;
- to monitor and protect the security (including network security) of OneCall24, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, customers and third parties*;
- to pay you and provide pension and other benefits in accordance with the contract between us and liaison with your pension provider or other providers of benefits*;
- paying tax and national insurance;
- to provide a reference upon request from another employer;

- to monitor your use of our information and communication systems to ensure compliance with our IT policies;
- to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
- to monitor compliance by you, us and others with our policies and our contractual obligations*;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;
- to conduct data analytics studies to review and better understand employee retention and attrition rates*;
- equal opportunities monitoring*;
- to answer questions from insurers in respect of any insurance policies which relate to you*;
- running, managing and planning our business, including but not limited to accounting and auditing;
- the prevention and detection of fraud or other criminal offences;
- to defend OneCall24 in respect of any investigation, litigation or accidents at work and to comply with any court or tribunal orders for disclosure; and
- for any other reason which we may notify you of from time to time.

We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting OneCall24's Head of Compliance.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity, subject to appropriate confidentiality safeguards.

We might process special categories of your personal data for the purposes in paragraph 7.2 above which have an asterisk beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws; and

- your sickness absence, health and medical conditions to monitor and manage your absence, assess your fitness for work, to provide you with or pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety.

We do not take automated decisions about you using your personal data or use profiling in relation to you.

1.8. Sharing your personal data

Sometimes we might share your personal data with pension and benefit providers, IT software and hardware providers, alarm and security companies, legal directories, medical professionals, group companies or our contractors and agents, stakeholders, suppliers and distributors to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

Third parties use your personal data to administer and process payroll, pension and benefits, to provide our IT systems and services, to administer other services for the business and to assist us with carrying out our obligations under our contract with you.

We may also use outsourced services in countries outside the European Union from time to time in other aspects of our business.

Accordingly, data obtained within the UK or any other country could be processed outside the European Union.

For example, some of the software our website uses may have been developed in the United States of America or in Australia.

We use the following safeguards with respect to data transferred outside the European Union:

- The data protection clauses in our contracts with data processors include transfer clauses written by or approved by a supervisory authority in the European Union.

1.9. How should you process personal data for the business?

Everyone who works for, or on behalf of, OneCall24 has some responsibility for ensuring data is collected, stored and handled appropriately.

OneCall24's Head of Compliance at the time of issuing this policy is Susanna Caddeo and is responsible for reviewing this policy. You should direct any questions in relation to this policy or data protection to this person.

You must comply with all the Detailed Policies which follow in this Privacy Policy concerning your use of IT systems and which comprise:

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

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of OneCall24 and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

You should not share personal data informally.

You should keep personal data secure and not share it with unauthorised people.

You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

You should use strong passwords.

You should lock your computer screens when not at your desk.

Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

Do not save personal data to your own personal computers or other devices.

Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the **Head of Compliance**.

You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

You should not take personal data away from OneCall24's premises without authorisation from your line manager.

Personal data should be shredded and disposed of securely when you have finished with it.

You should ask for help from the **Head of Compliance** if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure, and in sufficiently serious cases could be considered gross misconduct, which could result in your dismissal.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

1.10. How to deal with data breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact the **Head of Compliance** immediately and keep any evidence, you have in relation to the breach. See our separate GDPR Data Breach Policy, available from the **Head of Compliance**, for further details.

1.11. Subject access requests

Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request should be made in writing. If you receive such a request you should forward it immediately to the **Head of Compliance** who will coordinate a response.

If you would like to make a SAR in relation to your own personal data you should make this in writing to **Head of Compliance**. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request. For further details, see our separate GDPR Subject Access Request policy, available from the **Head of Compliance**.

1.12. Your data subject rights

You have the right to information about what personal data we process, how and on what basis as set out in this policy.

You have the right to access your own personal data by way of a subject access request (see above).

You can correct any inaccuracies in your personal data. To do so you should contact the **Head of Compliance.**

You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact the **Head of Compliance**.

While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the **Head of Compliance**.

You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

You have the right to object if we process your personal data for the purposes of direct marketing.

You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

With some exceptions, you have the right not to be subjected to automated decision-making.

You have the right to be notified of a data security breach concerning your personal data.

In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the **Head of Compliance**.

You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

1.13. DETAILED POLICIES

1.13.1 Email Acceptable Usage Policy.

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

- E-mails should be viewed as any other form of business communication. They should be polite and factual. Be aware that e-mails can be forwarded to other parties outside of your control.
- Take care in mentioning the names (or other identifying factors) of other employees and the employees of companies with whom we do business. They have their own rights of privacy – and if you are unsure, contact your manager or the Head of Compliance.
- Never attach any document to an e-mail (whether text, financial data or anything else) without it being first being encrypted using the encryption software provided for you to use.
- E-mails must not contain any swear words or phrases which could be considered offensive. Your line manager can provide further guidance as required.
- All e-mails should comply with our equal opportunities policy/anti-harassment policy. Remarks or jokes sent by e-mail can amount to harassment and, as with all harassment complaints, the intention of the party sending the e-mail is not relevant. E-mails 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 make personal or derogatory comments in e-mails.
- Do not tamper with anyone else's e-mail account. Specifically; do not send an e-mail which appears to originate from someone else but was typed by you.

- Do not forward someone else's e-mail for non-business-related reasons.
- Keep e-mails brief and business like.
- Avoid copying your colleagues into e-mails unnecessarily.

1.13.2 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.

1.13.3 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);
- breach confidentiality (for example, by revealing confidential intellectual property or information owned by OneCall24);
- discuss OneCall24's internal workings (such as agreements that it is reaching with partner institutions/customers or its future business plans that have not been communicated to the public);
- 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 (such as an employee of the 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 and Privacy Law (for example by naming other people and/or giving out details about them); 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 (such as agreements that it is reaching with partner institutions/customers or its future business plans that have not been communicated to the public);
- 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 (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 and Privacy Law (for example by naming other people and/or giving out details about them);
- fail to give acknowledgement where permission has been given to reproduce something.

1.13.4 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 the personal data that OneCall24 is responsible for remains within the control of OneCall24 at all times.
- 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 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. 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.

1.13.5 Business Application Policy.

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

1. Outlook
2. Microsoft Office
3. Visio
4. MS Project
5. Skype for Business
6. CRM
7. Google Chrome
8. WhatsApp
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

1.13.6 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.

2. GDPR Data Retention (England)

This section defines OneCall24's Data Retention Policy and is to be used in conjunction with OneCall24's Data Privacy section in this policy to adhere to the UK GDPR and Data Protection Act of 2018.

It sets the required retention periods for specified categories of personal data and sets out the minimum standards to be applied when destroying certain information within OneCall24.

The Policy consists of the following sections and applies to all staff without exception.

1. Retention Rules.
2. Safeguarding of Data during Retention Period.
3. Destruction of Data.
4. Breach, Enforcement and Compliance.
5. Document Disposal.
6. Appendix – Data Retention Schedule.

Adherence forms part of the employee's terms and conditions of employment and any breaches of policy may be considered a disciplinary offence and could lead to dismissal.

OneCall's Policy Lead Susanna Caddeo has overall responsibility for the Policy, its implementation and the effect it has on all staff.

2.1. Retention Rules.

OneCall24's GDPR Owner Matthew Betteridge defines the time period for which the documents and electronic records should to be retained through the Data Retention Schedule.

In the event, for any category of documents not specifically defined elsewhere in this Policy (and in particular within the Data Retention Schedule) and unless otherwise mandated differently by applicable law, the required retention period for such document will be deemed to be 10 years from the date of creation of the document.

As an exemption, retention periods within Data Retention Schedule can be prolonged in cases such as:

- Ongoing investigations from Member States authorities, if there is a chance records of personal data are needed by OneCall24 to prove compliance with any legal requirements; or
- When exercising legal rights in cases of lawsuits or similar court proceeding recognized under local law.

2.2. Safeguarding of Data during Retention Period.

The possibility that data media used for archiving will wear out shall be considered. If electronic storage media are chosen, any procedures and systems ensuring that the information can be accessed during the retention period (both with respect to the information carrier and the readability of formats) shall also be stored in order to safeguard the information against loss as a result of future technological changes. The responsibility for the storage falls to the GDPR Owner.

2.3. Destruction of Data.

OneCall24 and its employees will, on a regular basis, review all data, whether held electronically on their device or on paper, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant. See Appendix for the Data Retention Schedule. Overall responsibility for the destruction of data falls to the GDPR Owner.

Once the decision is made to dispose according to the Data Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal varies and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some expired or superseded contracts may only warrant in-house shredding. The Document Disposal section below defines the mode of disposal.

The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the GDPR Owner subcontracts for this purpose. Any applicable general provisions under relevant data protection laws and OneCall24's Data Protection Policy shall be complied with.

Appropriate controls shall be in place that prevents the permanent loss of essential information of OneCall24 as a result of malicious or unintentional destruction of information.

The GDPR Owner shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed.

2.4. Breach, Enforcement and Compliance.

The GDPR Owner has the responsibility to ensure that each of OneCall24's offices comply with this Policy. It is also the responsibility of the GDPR Owner to assist any local office with enquiries from any local data protection or governmental authority.

Any suspicion of a breach of this Policy must be reported immediately to GDPR Owner. All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate.

Failure to comply with this Policy may result in adverse consequences, including, but not limited to, loss of customer confidence, litigation and loss of competitive advantage, financial loss and damage OneCall24's reputation, personal injury, harm or loss. Non-compliance with this Policy by permanent, temporary or contract employees, or any third parties, who have been granted access to OneCall24 premises or information, may therefore result in disciplinary proceedings or termination of their employment or contract. Such non-compliance may also lead to legal action against the parties involved in such activities.

2.5. Document Disposal.

Records which may be routinely destroyed unless subject to an on-going legal or regulatory inquiry are as follows:

- Announcements and notices of day-to-day meetings and other events including acceptances and apologies.
- Requests for ordinary information such as travel directions.
- Reservations for internal meetings without charges / external costs.
- Transmission documents such as letters, fax cover sheets, e-mail messages, routing slips, compliments slips and similar items that accompany documents but do not add any value.
- Message slips.
- Superseded address list, distribution lists etc.
- Duplicate documents such as CC and FYI copies, unaltered drafts, snapshot printouts or extracts from databases and day files.
- Stock in-house publications which are obsolete or superseded.
- Trade magazines, vendor catalogues, flyers and newsletters from vendors or other external organizations.

In all cases, disposal is subject to any disclosure requirements which may exist in the context of litigation.
Confidential documents (i.e. those that contain information that is of the highest security and confidentiality and those that include any personal data) shall be disposed of as confidential waste (cross-cut shredded and incinerated) and shall be subject to secure electronic deletion.

Proprietary documents (i.e. those that contain confidential information such as parties' names, signatures and addresses, or which could be used by third parties to commit fraud, but which do not contain any personal data) should be cross-cut shredded and then placed into locked rubbish bins for collection by an approved disposal firm, and electronic documents will be subject to secure electronic deletion.

All other documents (i.e. those that Level do not contain any confidential information or personal data and are published OneCall24 documents) should be strip-shredded or disposed of through a recycling company and include, among other things, advertisements, catalogues, flyers, and newsletters. These may be disposed of without an audit trail.

If you require further information regarding any aspect of this policy, please contact your line manager.

Appendix – Data Retention Schedule

Financial Records

Personal data record category	Mandated retention period	Record owner
Payroll records	Ten years after audit	Finance
Supplier contracts	Ten years after contract is terminated	Finance
Chart of Accounts	Permanent	Finance
Fiscal Policies and Procedures	Permanent	Finance
Permanent Audits	Permanent	Finance
Financial statements	Permanent	Finance
General Ledger	Permanent	Finance
Investment records (deposits, earnings, withdrawals)	Seven years	Finance
Invoices	Seven years	Finance

Cancelled checks	Seven years	Finance
Bank deposit slips	Seven years	Finance
Business expenses documents	Seven years	Finance
Check registers/books	Seven years	Finance
Property/asset inventories	Seven years	Finance
Credit card receipts	Seven years	Finance
Petty cash receipts/documents	3 years	Finance

Business Records

Personal data record category	**Mandated retention period**	**Record owner**
Article of Incorporation to apply for corporate status	Permanent	Finance
Board policies	Permanent	Finance
Board meeting minutes	Permanent	Finance
Tax or employee identification number designation	Permanent	Finance
Office and team meeting minutes		Finance
Annual corporate filings	Permanent	Finance

HR: Employee and Candidate Records

Personal data record category	Mandated retention period	Record owner
Disciplinary, grievance proceedings records, oral/verbal, written, final warnings, appeals	As per legal requirement; for such period as required by policies or potential legal claim arising from same	HR
Applications for jobs, interview notes – Recruitment/promotion panel Internal: **Where the candidate is unsuccessful and has not been made compliant** **Where the candidate is successful**	 Archived as 'Do Not Use' after six months. Seven years after last assignment	HR
Payroll input forms, wages/salary records, overtime/bonus payments Payroll sheets, copies	Seven years after last assignment	HR
Bank details – current	Duration of employment	HR
Payrolls/wages	Duration of employment	HR
Job history including staff personal records: contract(s), Ts & Cs; previous service dates; pay and pension history, pension estimates, resignation/termination letters	Seven years after last assignment	HR
Employee address details	Seven years after last assignment	HR

Expense claims	As per legal requirement	HR
Annual leave records	Seven years after last assignment	HR
Accident books **Accident reports and correspondence**	As per legal requirement	HR
Certificates and self-certificates relating to Compliance and Competencies	Seven years after last assignment	HR
Pregnancy/childbirth certification	Seven years after last assignment	HR
Parental leave	Seven years after last assignment	HR
Maternity pay records and calculations	Seven years after last assignment	HR
Redundancy details, payment calculations, refunds, notifications	Seven years after last assignment	HR
Training and development records	Seven years after last assignment	HR
CRM data – inclusive of Name, Photo, Email address, mobile number, address, emails and phone call summaries, DPO information	Seven years after signing contract, compliance lapsing or request from Candidate to delete.	Registration & Compliance

Contracts

Personal data record category	Mandated retention period	Record owner
Signed	Permanent	Finance
Contract amendments	Permanent	Finance
Successful tender documents	Permanent	Finance
Unsuccessful tenders' documents	Permanent	Finance
Tender – user requirements, specification, evaluation criteria, invitation	Permanent	Finance
Contractors' reports	Permanent	Finance
Operation and monitoring, eg complaints	Permanent	Finance

Customer Data

Personal data record category	Mandated retention period	Record owner
CRM data – inclusive of Name, Email address, mobile number, address, emails and phone call summaries, DPO information	Seven years after last assignment or request from Customer to delete records.	Business Systems Administrator
Metrics data	Seven years after last assignment or request from Customer to delete.	Business Systems Administrator

Non – Customer Data

Personal data record category	Mandated retention period	Record owner
Name, email address	Kept until person unsubscribes / requests to be removed from system	Marketing & Sales

IT

Personal data record category	Mandated retention period	Record owner
Recycle Bins	Cleared monthly	Individual employee
Downloads	Cleared monthly	Individual employee
Inbox	All emails containing attachments deleted after three years.	Individual employee
Deleted Emails	Cleared monthly	Individual employee
Personal Network Drive	Reviewed quarterly, deleted after ten years.	Individual employee
Local Drives & files	Moved to network drive monthly, then deleted from local drive.	Individual employee

Shared Drives, Drop box	Reviewed quarterly, deleted after seven years.	Individual employee

3. GDPR Website Privacy Notice

This Document defines One Call 24's Website Privacy Notice and is to be used in conjunction with One Call 24's Data Privacy and Data Retention Policies to adhere to the UK GDPR (1st January 2021) and Data Protection Act of 2018.

The following text should be displayed on One Call 24's public website: https://onecall24.co.uk/

Privacy Notice

This is the privacy notice of OneCall24 Limited (herein referred to as "One Call 24", "we", "our", or "us"). We are registered as company number 09732799 in England and Wales. Our registered office is at 239 Old Marylebone Road, London, NW1 5QT.

As a trusted provider of healthcare professionals, we take our legal obligations very seriously. We respect your right to privacy and aim to be transparent at all times about our treatment of your information.

3.1. Introduction

This is a notice to inform you of our policy about all information that we record about you. It sets out the conditions under which we may process any information that we collect from you, or that you provide to us. It covers information that could identify you ("personal information") and information that could not. In the context of the law and this notice, "process" means collect, store, transfer, use or otherwise act on information.

We regret that if there are one or more points below with which you are not happy, your only recourse is to leave our website immediately.

We take seriously the protection of your privacy and confidentiality. We understand that all visitors to our website are entitled to know that their personal data will not be used for any purpose unintended by them and will not accidentally fall into the hands of a third party.

We undertake to preserve the confidentiality of all information you provide to us, and hope that you reciprocate.

Our policy complies with UK law accordingly implemented, including that required by the UK GDPR and Data Protection Act of 2018.

The law requires us to tell you about your rights and our obligations to you in regard to the processing and control of your personal data. We do this now, by requesting that you read the information provided at www.knowyourprivacyrights.org.

Except as set out below, we do not share, or sell, or disclose to a third party, any information collected through our website.

3.2. The bases on which we process information about you

The law requires us to determine under which of six defined bases we process different categories of your personal information, and to notify you of the basis for each category.

If a basis on which we process your personal information is no longer relevant, then we shall immediately stop processing your data.

If the basis changes then if required by law, we shall notify you of the change and of any new basis under which we have determined that we can continue to process your information.

3.3. Information we process because we have a contractual obligation with you

When you create an account on our website, buy a product or service from us, or otherwise agree to our terms and conditions, a contract is formed between you and us.

In order to carry out our obligations under that contract we must process the information you give us. Some of this information may be personal information.

We may use it in order to:

- Verify your identity for security purposes.
- Sell products to you.
- Provide you with our services.
- Provide you with suggestions and advice on products, services and how to obtain the most from using our website.

We process this information on the basis there is a contract between us, or that you have requested we use the information before we enter into a legal contract.

Additionally, we may aggregate this information in a general way and use it to provide class information, for example to monitor our performance with respect to a particular service we provide. If we use it for this purpose, you as an individual will not be personally identifiable.

We shall continue to process this information until the contract between us ends or is terminated by either party under the terms of the contract.

3.4. Information we process with your consent

Through certain actions when otherwise there is no contractual relationship between us, such as when you browse our website or ask us to provide you more information about our business, including job opportunities and our products and services, you provide your consent to us to process information that may be personal information.

Wherever possible, we aim to obtain your explicit consent to process this information, for example, by asking you to agree to our use of cookies.

Sometimes you might give your consent implicitly, such as when you send us a message by e-mail to which you would reasonably expect us to reply.

Except where you have consented to our use of your information for a specific purpose, we do not use your information in any way that would identify you personally. We may aggregate it in a general way and use it to provide class information, for example to monitor the performance of a particular page on our website.

If you have given us explicit permission to do so, we may from time to time pass your name and contact information to selected associates whom we consider may provide services or products you would find useful.

We continue to process your information on this basis until you withdraw your consent, or it can be reasonably assumed that your consent no longer exists.

You may withdraw your consent at any time by instructing us by sending an email to GDPR@onecall24.co.uk. However, if you do so, you may not be able to use our website or our services further.

3.5. Information we process for the purposes of legitimate interests

We may process information on the basis there is a legitimate interest, either to you or to us, of doing so.

Where we process your information on this basis, we do after having given careful consideration to:

- Whether the same objective could be achieved through other means.
- Whether processing (or not processing) might cause you harm.
- Whether you would expect us to process your data, and whether you would, in the round, consider it reasonable to do so.

For example, we may process your data on this basis for the purposes of:

- Record-keeping for the proper and necessary administration of our business.
- Responding to unsolicited communication from you to which we believe you would expect a response.
- Protecting and asserting the legal rights of any party.
- Insuring against or obtaining professional advice that is required to manage business risk.
- Protecting your interests where we believe we have a duty to do so.

3.6. Information we process because we have a legal obligation

We are subject to the law like everyone else. Sometimes, we must process your information in order to comply with a statutory obligation.

For example, we may be required to give information to legal authorities if they so request or if they have the proper authorisation such as a search warrant or court order.

This may include your personal information.

3.7. Specific uses of information you provide to us

3.7.1. Information provided relating to job applications, registration and employment

If you send us information in connection with a job application, we may keep it for up to ten years in case we decide to contact you at a later date.

If we employ you or register you so you can work at any of our client's, we collect information about you and the work you do from time to time. This information will be used only for purposes directly relevant to your employment. After your employment or registration has ended, we will keep your file for ten years before destroying or deleting it.

3.7.2. Information provided on the understanding that it will be shared with a third party

Our website allows you to post information with a view to that information being read, copied, downloaded, or used by other people.

Examples include:

- Referring a friend.
- Posting a message or tagging content after clicking on a link to a third-party website (e.g. Facebook, LinkedIn, Twitter, YouTube).
- Clicking on an icon next to another visitor's message to convey your agreement, disagreement or thanks after clicking on a link to a third-party website (e.g. Facebook, LinkedIn, Twitter, YouTube).

In posting personal information, it is up to you to satisfy yourself about the privacy level of every person who might use it. We do store it, and we reserve a right to use it in the future in any way we decide.

Once your information enters the public domain, we have no control over what any individual third party may do with it. We accept no responsibility for their actions at any time.

Provided your request is reasonable and there is no legal basis for us to retain it, then at our discretion we may agree to your request to delete personal information that you have posted. You can make a request by sending us an email at GDPR@onecall24.co.uk.

3.8. Complaints regarding content on our website

We attempt to moderate new website content, but we are not always able to do so as soon as that content is published.

If you complain about any of the content on our website, we shall investigate your complaint. If we feel it is justified or if we believe the law requires us to do so, we shall remove the content while we investigate.

Free speech is a fundamental right, so we have to make a judgment as to whose right will be obstructed: yours, or that of the person who posted the content that offends you.

If we think your complaint is vexatious or without any basis, we shall not correspond with you about it.

3.9. Information relating to payments and / or charges

Information relating to payment or charge arrangements is never taken by us or transferred to us through our website.

We store this information at your request the first time you provide it to us in order to make repeat use of our services more convenient.

We also store it to help us prevent fraud and restrict access to authorised staff only for your protection.

3.10. Information relating to communications with our support team

When you contact us, whether by telephone, through our website or by e-mail, we collect the data you have given to us in order to reply with the information you need.

We record your request and our reply in order to increase the efficiency of our organisation.

We keep personally identifiable information associated with your message, such as your name and email address so as to be able to track our communications with you to provide a high-quality service.

3.11. Complaining

When we receive a complaint, we record all the information you have given to us.

We use that information to resolve your complaint.

If your complaint reasonably requires us to contact some other person, we may decide to give to that other person some of the information contained in your complaint. We do this as infrequently as possible, but it is a matter for our sole discretion as to whether we do give information, and if we do, what that information is.

We may also compile statistics showing information obtained from this source to assess the level of service we provide, but not in a way that could identify you or any other person.

3.12. Affiliate and business partner information

This is information given to us by you in your capacity as an affiliate of us or as a business partner.

It allows us to recognise visitors that you have referred to us, and to credit to you commission due for such referrals. It also includes information that allows us to transfer commission to you.

The information is not used for any other purpose.

We undertake to preserve the confidentiality of the information and of the terms of our relationship.

We expect any affiliate or partner to agree to reciprocate this policy.

3.13. Use of information we collect through automated systems when you visit our website

3.13.1. Cookies

Cookies are small text files that are placed on your computer's hard drive by your web browser when you visit any website. They allow information gathered on one web page to be stored until it is needed for use on another, allowing a website to provide you with a personalised experience and the website owner with statistics about how you use the website so that it can be improved.

Some cookies may last for a defined period of time, such as one day or until you close your browser. Others last indefinitely.

Your web browser should allow you to delete any you choose. It also should allow you to prevent or limit their use.

Our website uses cookies. They are placed by software that operates on our servers, and by software operated by third parties whose services we use.

When you first visit our website, we ask you whether you wish us to use cookies. If you choose not to accept them, we shall not use them for your visit except to record that you have not consented to their use for any other purpose.

If you choose not to use cookies or you prevent their use through your browser settings, you will not be able to use all the functionality of our website.

We use cookies in the following ways:

- To track how you use our website.
- To record whether you have seen specific messages we display on our website.
- To record your answers to surveys and questionnaires on our site while you complete them

We provide more information about the cookies we use in our Cookie Policy.

3.13.2. Personal identifiers from your browsing activity

Requests by your web browser to our servers for web pages and other content on our website are recorded.

We record information such as your geographical location, your Internet service provider and your IP address. We also record information about the software you are using to browse our website, such as the type of computer or device and the screen resolution.

We use this information in aggregate to assess the popularity of the webpages on our website and how we perform in providing content to you.

If combined with other information we know about you from previous visits, the data possibly could be used to identify you personally, even if you are not signed in to our website.

3.13.3. Our use of re-marketing

Re-marketing involves placing a cookie on your computer when you browse our website in order to be able to serve to you an advert for our products or services when you visit some other website.

We may use a third party to provide us with re-marketing services from time to time. If so, then if you have consented to our use of cookies, you may see advertisements for our products and services on other websites.

3.14. Disclosure and sharing of your information

3.14.1. Information we obtain from third parties

Although we do not disclose your personal information to any third party (except as set out in this notice), we sometimes receive data that is indirectly made up from your personal information from third parties whose services we use.

No such information is personally identifiable to you.

3.14.2. Credit references

To assist in combating fraud, we share information with credit reference agencies, so far as it relates to clients or customers who instruct their credit card issuer to cancel payment to us without having first provided an acceptable reason to us and given us the opportunity to refund their money.

3.15. Data may be processed outside the European Union

Our website is hosted in the European Union. We may also use outsourced services in countries outside the European Union from time to time in other aspects of our business.

Accordingly, data obtained within the UK or any other country could be processed outside the European Union.

For example, some of the software our website uses may have been developed in the United States of America or in Australia.

We use the following safeguards with respect to data transferred outside the European Union:

- The data protection clauses in our contracts with data processors include transfer clauses written by or approved by a supervisory authority in the European Union.

3.16. Access to your own information

3.16.1. Access to your personal information

At any time, you may review or update personally identifiable information that we hold about you, by sending us a Subject Access Request (SAR).

To obtain a copy of any information that is not provided on our website you may send us a request by emailing us at GDPR@onecall24.co.uk and requesting a Subject Access Request form. You should then compete the form and send it marked "For the attention of OneCall24's Head of Compliance" by registered post to our registered address.

After receiving the request, we will tell you when we expect to provide you with the information, and whether we require any fee for providing it to you.

3.16.2. Removal of your information

If you wish us to remove personally identifiable information we hold about you, you may send us a request by emailing us at GDPR@onecall24.co.uk and requesting a Subject Access Request form. You should then compete the form and send it marked "For the attention of OneCall24's Head of Compliance" by registered post to our registered address.

This may limit the service we can provide to you.

3.16.3. Verification of your information

When we receive any request to access, edit or delete personal identifiable information we shall first take reasonable steps to verify your identity before granting you access or otherwise taking any action. This is important to safeguard your information.

3.17. Other matters

3.17.1. Use of site by children

We do not sell products or provide services for purchase by children, nor do we market to children.

If you are under 18, you may use our website only with consent from a parent or guardian

We collect data about all users of and visitors regardless of age, and we anticipate that some of those users and visitors will be children.

Such child users and visitors will inevitably visit other parts of the site and will be subject to whatever on-site marketing they find, wherever they visit.

3.17.2. How you can complain

If you are not happy with our privacy policy or if have any complaint, then you should tell us by email. Our address is GDPR@onecall24.co.uk.

If a dispute is not settled, then we hope you will agree to attempt to resolve it by engaging in good faith with us in a process of mediation or arbitration.

If you are in any way dissatisfied about how we process your personal information, you have a right to lodge a complaint with the Information Commissioner's Office. This can be done at https://ico.org.uk/concerns/

3.17.3. Retention period for personal data

Except as otherwise mentioned in this privacy notice, we keep your personal information only for as long as required by us:

- To provide you with the services you have requested.
- To comply with other law, including for the period demanded by our tax authorities.
- To support a claim or defence in court

3.17.4. Compliance with the law

Our privacy policy has been compiled so as to comply with the law of every country or legal jurisdiction in which we aim to do business. If you think it fails to satisfy the law of your jurisdiction, we should like to hear from you.

However, ultimately it is your choice as to whether you wish to use our website.

3.17.5. Review of this privacy policy

We may update this privacy notice from time to time as necessary. The terms that apply to you are those posted here on our website on the day you use our website. We advise you to print a copy for your records.

If you have any question regarding our privacy policy, please contact us.

3.18. GDPR Data Breach Policy

This document defines OneCall24's Data Breach Policy ("Policy") and is to be used in conjunction with OneCall24's Data Privacy and Retention Policies to adhere to the UK GDPR and Data Protection Act of 2018.

Data security breaches are increasingly common occurrences whether caused through human error or via malicious intent. As the amount of data and information grows and technology develops, there are new ways by which data can be breached. OneCall24 needs to have a robust and systematic way of responding to any reported data security breach, to ensure it can act responsibly and protect personal data which it holds.

The Policy consists of the following sections :

7. Introduction.
8. Responsibility.
9. Our duties.
10. What can cause a personal data breach?
11. If you discover a personal data breach.
12. Managing and reporting the breach.
13. Monitoring and review.
14. Staff awareness and training.
15. Reporting concerns.
16. Consequences of non-compliance.

3.18.1. Introduction

This Data Breach Policy:

- places obligations on staff to report actual or suspected personal data breaches; and
- sets out our procedure for managing and recording actual or suspected breaches.

This plan applies to all staff in the UK and to all personal data and special category personal data held by One Call 24 Limited ("OneCall24"). This plan supplements our other policies relating to data protection privacy, retention and subject access requests.

The table below explains some key terminology used in this plan:

Term	**Meaning**
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed—e.g. accidental loss, destruction, theft, corruption or unauthorised disclosure of personal data.
Personal data	Information relating to an individual who can be identified (directly or indirectly) from that information.
Data subject	The individual to whom the personal data relates.
Special category personal data (sometimes known	Personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information

Term	Meaning
as sensitive personal data)	(where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.
Policy Lead	The person we appoint from time to time to lead all aspects of the development and implementation of our data protection and data privacy strategy and compliance with the GDPR and other applicable laws.
Data breach team	The team responsible for investigating personal data breaches.
Information Commissioner's Office (ICO)	The UK's independent data protection and information regulator.

3.18.2. Responsibility

OneCall24's Policy Lead Susanna Caddeo has overall responsibility for this Policy. They are responsible for ensuring it is adhered to by all staff.

3.18.3. Our duties

OneCall24 processes personal data relating to individuals including staff, clients and third parties. As custodians of data, we have a responsibility under the UK General Data Protection Regulation (GDPR) to protect the security of the personal data we hold.

We must keep personal data secure against loss or misuse. All staff are required to comply with our security guidelines and policies (in particular our GDPR Data Privacy and Data Retention Policies).

3.18.4. What can cause a personal data breach?

A personal data breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored, e.g. loss of a laptop or a paper file.
- Inappropriate access controls or sharing allowing unauthorised use.
- Equipment failure, fire or flood.
- Human error, e.g. sending an email or SMS to the wrong recipient.
- Unforeseen circumstances such as a fire or flood.
- Hacking, phishing, malware and other 'blagging' attacks where information is obtained by deceiving whoever holds it.
- Information obtained by deception.
- Non-secure disposal of data,
- Unescorted visitors accessing data.

3.18.5. If you discover a personal data breach

If you know or suspect a personal data breach has occurred or may occur, you should:

- complete a Data Breach Incident Report form. The form asks for your name, but you do not have to give it if you would prefer to report the failure anonymously;
- email the completed form to the Head of Compliance at GDPR@onecall24.co.uk—if you wish to make an anonymous report, you can submit the form by a non-electronic method, e.g. internal post to the Head of Compliance;
- telephone the Head of Compliance to let them know a form has been (or is being) completed on 0333 221122.

Where appropriate, you should liaise with your line manager about completion of the Data Breach Incident Report form. However, this may not be appropriate or possible, e.g. if your line manager is aware of the breach and has instructed you not to report it, or if they are simply not available. In these circumstances, you should submit the report directly to the Head of Compliance without consulting your line manager.

You should not take any further action in relation to the breach. In particular, you must not notify any affected individuals or regulators. The Head of Compliance will acknowledge receipt of the data breach report form (if the person making the report has given their name) and take appropriate steps to deal with the report in collaboration with the data breach team.

3.18.6. Managing and recording the breach

On being notified of a suspected personal data breach, the Head of Compliance will establish a data breach team. The data breach team will be led by the Head of Compliance.

The data breach team will take immediate steps to establish whether a personal data breach has, in fact, occurred. If so, the data breach team will take appropriate action to:

- contain the data breach and (so far as reasonably practicable) recover, rectify or delete the data that has been lost, damaged or disclosed;
- assess and record the breach in OneCall24's data breach register;
- notify appropriate parties of the breach;
- take steps to prevent future breaches.These are explained in paragraphs 6.3 to 6.6.

3.18.7. Containment and recovery

The data breach team will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data.

The data breach team will identify ways to recover, correct or delete data. This may include contacting the police, e.g. where the breach involves stolen hardware or data.

Depending on the nature of the breach, the data breach team will notify our insurers as the insurers can provide access to data breach management experts.

3.18.8. Assess and record the breach

Having dealt with containment and recovery (see paragraph 3.18.7), the data breach team will assess the risks associated with the breach, including:

- what type of data is involved?
- how sensitive is the data?
- who is affected by the breach, ie the categories and approximate number of data subjects involved?
- the likely consequences of the breach on affected data subjects, e.g. what harm can come to those individuals, are there risks to physical safety or reputation, or financial loss?
- where data has been lost or stolen, are there any protections in place such as encryption or pseudonymisation?
- what has happened to the data, e.g. if data has been stolen, could it be used for harmful purposes?
- what could the data tell a third party about the data subject, e.g. could the loss of apparently trivial snippets of information help a determined fraudster build up a detailed picture of other people?
- what are the likely consequences of the personal data breach on OneCall24, e.g. loss of reputation, loss of business, liability for fines?
- are there wider consequences to consider, e.g. loss of public confidence in an important service we provide?

Details of the breach will be recorded in OneCall24's data breach register by the data breach team.

3.18.9. Notifying appropriate parties of the breach

The data breach team will consider whether to notify:

- the ICO
- affected data subjects
- the police
- any other parties, e.g. insurers or commercial partners

3.18.10. Notifying the ICO

The data breach team will notify the ICO when a personal data breach has occurred, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

Where ICO notification is required, this shall be done without undue delay and, where feasible, not later than 72 hours after we became aware of it. Where the notification to the ICO is not made within 72 hours, it will be accompanied by reasons for the delay.

If the data breach team is unsure whether or not to report, the presumption should be to report. The data breach team will take account of the factors set out below:

The potential harm to the rights and freedoms of data subjects	This is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include: • exposure to identity theft through the release of non-public identifiers, e.g. passport number • information about the private aspects of a person's life becoming known to others, e.g. financial circumstances *The personal data breach must be reported unless it is unlikely to result in a risk to data subjects' rights and freedoms.*
The volume of personal data	There should be a presumption to report to the ICO where: • a large volume of personal data is concerned, and • there is a real risk of individuals suffering some harm It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances of the loss or the extent of information about each individual. The ICO provides two examples: • loss of an unencrypted laptop holding names, addresses, dates of birth and National Insurance numbers of 100 individuals would be reportable • loss of a marketing list of 100 names and addresses (or other contact details) where there is no particular sensitivity of the service being marketed would not be reportable**]**
The sensitivity of data	There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress. This is most likely to be the case where the breach involves special category personal data. If the information is particularly sensitive, even a single record could trigger a report. The ICO provides two examples: • theft of a manual paper-based filing system (or unencrypted digital media) holding the personal data and financial records of 50 named individuals would be reportable • breach of a similar system holding the trade union subscription records of the same number of individuals (where there are no special circumstances surrounding the loss, the koss would not be reportable**)**

3.18.11. Notifying data subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data breach team will notify the affected data subject(s) without undue delay, including:

- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- the likely consequences of the personal data breach;
- the measures we have or intend to take to address the personal data breach, including, where appropriate, recommendations for mitigating potential adverse effects.

When determining whether and how to notify data subjects of the breach, the data breach team will

- co-operate closely with the ICO and other relevant authorities, e.g. the police; and
- take account of the factors set out in the table below:

Factor	**Impact on obligation to notify data subject**
Whether we have implemented and applied (to the affected personal data) appropriate technical and organisational protection measures—in particular measures that render the personal data unintelligible to any person who is not authorised to access it, e.g. encryption.	Where such measures have been implemented, it is not necessary to notify the data subject(s).
Whether we have taken measures following the personal data breach which ensure the high risk to the rights and freedoms of data subjects affected by that breach is no longer likely to materialise.	Where such measures have been implemented, it is not necessary to notify the data subject(s).
Whether it would involve disproportionate effort to notify the data subject(s).	If so, it is not necessary to notify the data subject(s)—but we must, instead, issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
Whether there are any legal or contractual requirements to notify the data subject?	If yes, it may be necessary to notify the data subject(s) in any event.

3.18.12. Notifying the police

The data breach team will already have considered whether to contact the police for the purpose of containment and recovery (see paragraph 3.18.7). Regardless of this, if it subsequently transpires that the breach arose from a criminal act perpetrated against or by a representative of OneCall24, the data breach team will notify the police and/or relevant law enforcement authorities.

3.18.13. Notifying other parties

The data breach team will consider whether there are any legal or contractual requirements to notify any other parties, e.g. such are any regulatory bodies or our insurers.

3.18.14. Preventing future breaches

Once the personal data breach has been dealt with, in accordance with this plan, the data breach team will:

- establish what security measures were in place when the breach occurred
- assess whether technical or organisational measures can be implemented to prevent the breach happening again
- consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice
- consider whether it is necessary to update our privacy risk assessment
- update OneCall24's privacy risk register
- debrief data breach team members following the investigation

3.18.15. Monitoring and review

1.2 We will monitor the effectiveness of all our policies and procedures regularly, and conduct a full review and update as appropriate, at least [every two years].

1.3 Our monitoring and review exercises will include looking at how our policies and procedures are working in practice to reduce the risks posed to our company.

3.18.16. Staff awareness and training

Key to the success of our systems is staff awareness and understanding.

We provide regular training to staff:

- at induction
- when there is any change to the law, regulation or our policy
- when significant new threats are identified
- in the event of an incident affecting our company or a competitor

3.18.17. Reporting concerns

Prevention is always better than cure. Data security concerns may arise at any time and we encourage you to report any concerns you have to the Head of Compliance. This helps us capture risks as they emerge, protect our company from personal data breaches, and keep our processes up-to-date and effective.

3.18.18. Consequences of non-compliance

Failure to comply with this plan and associate data protection policies puts you and OneCall24 at risk. Failure to notify the Head of Compliance of an actual or suspected personal data breach is a very serious issue.

You may be liable to disciplinary action if you fail to comply with the provisions of this, and all related plans, policies and procedures.