OCS
One Care Solution
We care for you

GDPR Data Privacy Policy for Agency Workers

Policy Number	20
Version	4
Policy Contact	Demoiselle Chidzuu
Date Issued	21st May 2018
Reviewed	01st June 2023
Next Review Date	01st June 2024
Target Audience	Staff and Consultants
Approved by	ONECS Policy Team

This Document defines ONECS's Data Privacy Policy for Agency Workers ("Privacy Policy") and is to be used to adhere to the UK GDPR and Data Protection Act of 2018.

It 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. Subject access requests;
12. Your data subject rights;

and the following Detailed Policies

13. Email Acceptable Usage Policy.
14. Internet Acceptable Usage Policy.
15. Social Media Acceptable Use Policy.
16. Infrastructure Monitoring Policy.

1 Overview

1.1 ONECS Limited (co. reg. no. 11768842 of 166 High Street East Wallsend Newcastle Upon Tyne ("ONECS") 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.

1.2 This policy applies to all agency workers of ONECS. 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.

1.3 ONECS 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.

1.4 ONECS 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.

1.5 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, ONECS.

2 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 2018 Act and the GDPR. If any conflict arises between those laws and this policy, we intend to comply with the UK GDPR and Data Protection Act of 2018.

3 Data Protection Principles

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

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

4 How we define personal data

4.1 '**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.

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

4.3 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.

4.4 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.

5 How we define special categories of personal data

5.1 '**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.

6 How we define processing

6.1 **'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.

7 How will we process your personal data?

7.1 ONECS will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

7.2 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.

8 Examples of when we might process your personal data

8.1 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).

8.2 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 ONECS, 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 ONECS 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.

8.3 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 **ONECS's Head of Compliance**.

8.4 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.

8.5 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.

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

9 Sharing your personal data

9.1 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.

9.2 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.

9.3 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.

9.4 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.

10 How should you process personal data for the business?

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

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

10.3 You should 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.

10.4 You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of ONECS 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.

10.5 You should not share personal data informally.

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

10.7 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.

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

10.9 You should use strong passwords.

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

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

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

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

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

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

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

10.17 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.

10.18 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.

10.19 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.

11 How to deal with data breaches

11.1 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.

11.2 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.

12 Subject access requests

12.1 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.

12.2 If you would like to make a SAR in relation to your own personal data, you should make this in writing to the **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.

12.3 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**.

13 Your data subject rights

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

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

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

13.4 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**.

13.5 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**.

13.6 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.

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

13.8 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.

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

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

13.11 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**.

13.12 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.

DETAILED POLICIES

14 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.

15 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 ONECS'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.

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

ONECS 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 agency workers duty of fidelity to ONECS (for example, emailing confidential information of ONECS to a competitor), the agency worker 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 ONECS the breach may be treated as grounds for dismissal.

16 Social Media Acceptable Use Policy.

Any communications that agency workers **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 ONECS).
- discuss ONECS'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 ONECS);

- post images or links to content that could be considered inappropriate, discriminatory or offensive;
- bring ONECS 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 ONECS);
- give away confidential information about an individual (such as a colleague or partner contact) or organisation (such as a partner institution);
- discuss ONECS'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 ONECS 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.

17 Infrastructure Monitoring Policy.

OneCall24 recognise agency workers right to privacy and our responsibilities under law. In particular:

- We recognise that agency workers have a right to privacy in respect of their personal communications.
- We reserve the right to monitor agency workers use of e-mail and the Internet to ensure compliance with ONECS'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, ONECS 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 agency worker 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 ONECS'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 agency worker as soon as practical – this may be as part of an investigation conducted under ONECS's disciplinary process.

ONECS 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 agency workers, and the email addresses of those with whom they have communicated.

ONECS may engage in real-time surveillance of Internet usage, monitor the content of email messages sent or received by its agency workers unless a copy of such message is sent or forwarded to ONECS 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.

Review

This policy statement will be reviewed annually as part of our commitment to upholding professional standards. It may be altered from time to time in the light of legislative changes, operational procedures or other prevailing circumstances.