National Centre for Social Research

Third party agreement

Companies

This document forms NatCen's standard terms. They may be varied for specific projects subject to agreement by NatCen's Head of Information Security or Director of Information Technology. Any variations must be documented and appended to the agreement.

The document is divided into three parts and is valid for a period of 3 years from the date when it is signed.

Part A: Mandatory requirements for processors of personal data (UK GDPR)

The UK General Data Protection Regulation (UK GDPR) sets out key principles for the management of personal data, gives people control over how their information is used and imposes significant fines on data controllers and data processors who do not comply.

For us here at NatCen, the UK GDPR reinforces the principles we live by. We will continue to work in a lawful, fair and transparent manner, meaning personal data will be accurate, completely confidential, only collected for legitimate purposes and only stored for the required amount of time.

This Part therefore sets out the minimum requirements regarding access to and the processing of NatCen information. The UK GDPR allows us to use only processors who provide sufficient guarantees that they implement appropriate technical and organisational measures in such a manner as to ensure that processing will meet the requirements of UK GDPR and ensure the protection of the rights and freedoms of data subjects. We cannot engage any supplier to process personal data on our behalf who is unable to fulfil these requirements and this 'Agreement' shall remain in force for as long you / your company has access to that information.

1. Only processing data in accordance with written instructions

You shall process personal data only on documented instructions from NatCen, except where you are required to do otherwise by UK law to which NatCen is subject. In such a case, you shall inform NatCen of that legal requirement before processing, unless that law prohibits you from doing so on important grounds of public interest.

You shall take steps to ensure that anyone acting under your authority who has access to personal data does not process them except on instructions from NatCen, unless he or she is required to do so by UK law.

2. Ensuring confidentiality amongst staff

You shall ensure that anyone you authorise to process data on NatCen's behalf has committed themselves to confidentiality or is under an appropriate statutory obligation of confidentiality.

3. Ensuring processing is secure

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk and severity for the rights and freedoms of natural persons, you shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This will include:

1. the pseudonymisation and encryption of personal data
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

In assessing the appropriate level of security, you shall take into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

4. Responding to requests arising from the exercise of data subjects' rights

When requested, and taking into account the nature of the processing we have asked you to carry out, you shall assist NatCen by appropriate technical and organisational measures, insofar as this is possible, to fulfil our obligation to respond to requests to exercise the data subjects' rights laid down in Chapter III of UK GDPR.

5. Notifying NatCen of any personal data breaches

In the case of a personal data breach, you shall without undue delay and not later than 24 hours after having become aware of it notify NatCen of that breach, whether or not you have yet finished investigating or resolving it. Please note, NatCen and our customers have only 72 hours from the time you first become aware of the breach before potentially reporting it to the Information Commissioner's Office so cannot afford for you to use up much of that time.

The notification shall describe at least:

1. the nature of the personal data breach including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
2. the name and contact details of the Data Protection Officer or other contact point where more information can be obtained
3. the likely consequences of the personal data breach
4. the measures taken or proposed to be taken by you to address the breach, including where appropriate measures to mitigate its possible adverse effects

You shall assist NatCen in determining whether the data breach is likely to result in a risk to the rights and freedoms of natural persons.

NatCen will document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

6. Carrying out data protection impact assessments

If you carry out processing using new technologies, and where the nature, scope, context and purposes of the processing are likely to result in a high risk to the rights and freedoms of natural persons, you shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data before processing it in any way.

The data protection impact assessment shall contain at least:

1. a systematic description of the envisaged processing operations and the purposes of the processing
2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes
3. an assessment of the risks to the rights and freedoms of data subjects
4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with UK GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned

You shall carry out a review to determine whether processing is performed in accordance with the data protection impact assessment whenever there is a change to the risk represented by processing operations.

7. Data deletion

You shall delete all personal data or return it to NatCen at the end of the provision of services, and you shall delete all copies unless UK law requires its storage.

8. Demonstrating compliance

If requested, you shall make available to NatCen all information necessary to demonstrate your compliance with this agreement and the requirements of UK GDPR, and you shall allow for and contribute to audits, including inspections, conducted by NatCen or another auditor mandated by NatCen.

You shall inform NatCen immediately if, in your opinion, an instruction infringes UK GDPR or other UK data protection provisions.

9. Engaging a sub-processor

You shall not engage another processor without prior specific or general written authorisation from NatCen. In the case of general written authorisation, you shall inform NatCen of any intended changes concerning the addition or replacement of other processors, thereby giving NatCen the opportunity to object to such changes.

Where you engage another processor to carry out specific processing activities on NatCen’s behalf, the same data protection obligations as set out in this agreement shall be imposed by you on that other processor by way of a contract or other legal act, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of ISO 27001 and UK GDPR. Where that other processor fails to fulfil its data protection obligations, you shall remain fully liable to NatCen for the performance of that other processor's obligations.

Part B: Additional requirements

Part B contains requirements arising from ISO 27001 and best practice more widely. NatCen is certified to the ISO 27001 Information Security Management System standard, which means that NatCen requires third parties that process personal or confidential data on our behalf to demonstrate and provide evidence that they comply with the best practice principles defined in ISO 27001.

If there are any requirements stated in this Part which you are unable to fulfil then please list them in the table in Part C, stating why you cannot fulfil them and whether there are any alternative measures you have in place.

10. Information security policy

NatCen expects that you have an up-to-date formal documented information security policy applicable to your processing, storage or handling of NatCen information. You must supply NatCen with evidence of this policy and describe precisely how it applies to NatCen information (see Part C).

11. Organising information security

NatCen expects you to provide the name, role, telephone number and email address of the person responsible for information security within your organisation. Their position must carry appropriate authority within the general management structure of the organisation.

NatCen expects that all staff handling NatCen information have been trained on information security and the non-disclosure agreements (see Appendix 1) have been signed. You should retain these and make them available for audit by NatCen if requested.

12. Information asset management

Physical assets which handle NatCen information must:

- have a nominated owner
- be identifiable and traceable
- have their details logged

NatCen information must be given appropriate protection and all staff handling the information must be informed how to protect this information.

Access to NatCen information must be strictly controlled and only people with a justifiable reason to access NatCen's information should have access to it, whether in paper or electronic form. NatCen information must never be taken off site without NatCen's specific authorisation.

All paper documentation containing personal details such as names and addresses must be subject to clear desk policy, locked away when not in use and always sent via recorded or registered post if required. Information containing personal details must never be faxed. Specific handling arrangements for paper documents must be agreed with the NatCen Project Manager in advance.

All mobile computers that are used to hold or process personal or confidential information must be protected with full disk encryption to at least a minimum of FIPS 140-2. All mobile computers that are used to hold or process NatCen information must have access control implemented and up-to-date anti-virus protection installed. NatCen information stored on mobile computers must be kept to the absolute minimum needed to support the business processes or project.

All use of removable media in respect of NatCen information must be specifically authorised by NatCen. All removable media such as CDs, DVDs, removable hard drives or USB sticks used to store NatCen information must be encrypted to a minimum of FIPS 140-2.

Strict procedures for the destruction of NatCen information must be agreed in advance with the NatCen Project Manager. On completion of the assignment all documentation and physical media must be either returned to

NatCen or permanently deleted from any computer used for working on the project. Data deletion of confidential or personal data must be to the US DoD (7-pass) standard.

13. Transferring data

All electronic data sent by email or on electronic media must be encrypted in transit (this must be at least 256-bit AES encryption or FIPS 140-2 where contractually required). The method of transmitting and receiving NatCen data must be specifically agreed with the NatCen Project Manager in advance.

14. Human resources

NatCen expects the following checks to be carried out for all staff with access to NatCen information:

- Identity validation
- Employment history (past 3 years)
- Nationality and immigration status
- Additionally, prospective employees are required to give a reasonable account of any significant periods (six months or more in the past three years) of time spent abroad

You are also required to ensure that all staff with access to NatCen information:

- Sign the non-disclosure agreement (Appendix 1)
- Are properly trained
- Are made aware of their security responsibilities
- Are made aware of their legal responsibilities
- Are reminded of ongoing security and legal responsibilities on termination of employment
- Are informed that they must report any security weaknesses that they identify to your company security representative for reporting to NatCen and resolution

In addition NatCen reserves the right to require that criminal record checks (unspent convictions only) are carried out for staff working on certain projects.

All access to NatCen information must be removed immediately when access is no longer required.

15. Physical and environmental security

Only authorised personnel should have access to sites, buildings and offices holding NatCen information with additional controls in place for secure areas.

If physical access tokens such as swipe cards are used then they must be managed to ensure that only staff with a legitimate and ongoing requirement are in possession of such a token.

Procedures must be in place to ensure that staff are informed that they must:

- Hold all physical access tokens securely at all times
- Report the loss or theft of a physical access token immediately
- Supervise visitors at all times

All hardware handling or storing NatCen information must be maintained in accordance with the manufacturer's specifications. All equipment used to process or store NatCen information must be protected to prevent loss of information. Full back-up and disaster recovery plans must be in place for all systems and equipment used to process NatCen information. NatCen must be consulted before any equipment containing NatCen information is either disposed of or destroyed.

Access to NatCen information must be strictly controlled. All servers holding NatCen information must be held in secure rooms with strictly controlled access. Access to physical media and documentation must also be strictly controlled. NatCen physical information and documentation must always be held in locked storage when not attended.

16. Communication & operations security

NatCen expects that good operations and network management controls are established. These controls must cover logical access; vulnerability analysis; firewall controls; lifestyle devices controls; and remote working.

Clear work instructions or procedures must be available for all systems and services handling NatCen information to ensure their correct and secure live running.

Any test and development environments must be segregated on all systems processing NatCen information. NatCen information must never be used for testing purposes.

Systems and services storing or processing NatCen information must implement anti-virus measures, including patching, in accordance with the manufacturers' recommendations.

Formal back-up procedures must be in place to prevent the loss or corruption of NatCen information. Back-up systems must be tested with evidence of successful restore after testing.

Written procedures must be implemented to control the use of back-up data in respect of NatCen information. Use of NatCen data that has been backed up must always be authorised by the NatCen Project Manager or NatCen Head of Information Security.

17. Logical access control

NatCen expects that a hierarchy of logical access control mechanisms are in place. These controls cover access to operations, systems and applications containing NatCen information.

The written access control policy must ensure that access is:

- Limited at an individual level to those functions needed to perform appropriate business functions
- Removed, at an individual user level, immediately access is no longer required to that information
- Only provided to the minimum number of users
- Only granted when formally approved
- Recorded formally for all users

Where a physical security token is used as part of the logon process there must be clearly defined and documented procedures for the use of that token.

Output containing NatCen information must only be sent to locations approved by NatCen.

All systems and services handling NatCen information must have a clearly defined set of password rules to include:

- A minimum password length of 10 characters;
- It must comprise of characters from 3 of the following 4 categories:
    - a-z lower case
    - A-Z upper case
    - Numeric 0-9
    - Special character, such as punctuation
- No more than 2 consecutive characters can be the same
- Must not be the same as the user name
- Must be changed every 30 days

The mechanisms provided for enabling, disabling, modifying or deleting user registration details must only be accessible to authorised individuals in line with the access control policy. System administrators must not logon with full supervisor privileges unless it is essential to do so.

All networks containing NatCen information, including any supplied by a third party to the contractor, must be managed to ensure:

- User access is controlled
- Links to other networks are authenticated before the link is established
- Remote diagnostic ports are securely managed and controlled

All detected unauthorised access (or attempted access) must be treated as a security incident.

It must be possible to identify all users with access to NatCen information and trace their actions.

18. Information systems acquisition, development and maintenance

NatCen expects that access to all systems containing NatCen information in relation to maintenance, repair or replacement of equipment is strictly controlled. This includes temporary access granted either directly or indirectly to engineers or external support services.

19. Information audit

All systems and processes involving the receipt and despatch of NatCen personal or other confidential information must provide an audit trail for sensitive information which can be interrogated by authorised individuals and will identify who has:

- browsed information
- created information
- updated information
- deleted information

The audit trail will include date and time stamps for all events, and the source location of where the event was triggered from.

The audit trail must be checked regularly and any unpredicted events reported to NatCen.

20. Information security incident management

There must be a documented process for handling security incidents within your organisation with nominated staff having specific responsibility for investigating and reporting incidents.

There must be a formal disciplinary process defined for people who cause security incidents.

The NatCen Project Manager and the NatCen Head of Information Security must be informed straight away of any security incidents relating to processing, storage or handling of NatCen information. These include but are not limited to unauthorised access, denial of service, loss of information and data corruption.

All staff handling NatCen information must be informed how to:

- Recognise a security incident
- Report a security incident
- Where appropriate, investigate and report a security incident

21. Business continuity management

A Business Continuity Plan must be in place to ensure that in the event of business continuity being invoked data loss is minimised. NatCen should be immediately advised of the event and of the recovery plans for restoring, protecting and delivering NatCen information.

22. Compliance

Evidence of your organisation's compliance with relevant statutory, regulatory, contractual, copyright and intellectual standards, regulations and legislation applicable to your handling of NatCen's information must be available for inspection.

These should include but not be limited to your Data Protection Act registration and any evidence of compliance to information security standards such as ISO 27001.

All work in relation to NatCen data must comply with the UK General Data Protection Regulation and the Data Protection Act 2018.

Part C: Evidence and confirmation

YOU ARE REQUIRED TO FILL OUT THIS PART AND RETURN TO:

Head of Information Security
National Centre for Social Research (NatCen)
Kings House
101-135 Kings Road, Brentwood, CM14 4LX

Evidence of Information Security Policy	
Please attach a copy of your policy or provide a link to its location on your website	

Person responsible for information security	
Name	
Role / job title	
Telephone number	
Email address	

Exceptions

You must fulfil all the requirements set out in Part A. If there are any aspects of the requirements in Part B which you are unable to fulfil then please list them in the table below, stating why you cannot fulfil them and whether there are any alternative measures you have in place.

The requirement we cannot fulfil is...	The reason we cannot fulfil this requirement is... Alternative measures we have in place are...

Confirmation

I confirm that the work undertaken on behalf of NatCen will be undertaken in accordance with the principles and standards defined within this document.

Organisation name	
Name	
Role / job title	
Telephone number	
Email address	
Signature	
Date	

Appendix 1

THIS DOCUMENT SHOULD BE SIGNED BY ALL STAFF HANDLING NATCEN INFORMATION AND RETAINED BY YOU. THESE SIGNED FORMS SHOULD BE MADE AVAILABLE TO NATCEN UPON REQUEST.

NatCen non-disclosure agreement

Whilst working with NatCen I confirm that I agree to the principles and standards defined within this document.

I shall not at any time, directly or indirectly, use, divulge or communicate any trade secrets, technical or confidential information relating to or belonging to NatCen which I may have received or obtained whilst working with NatCen.

This information includes any information relating to the operation of the organisation, in particular respondents' and clients' details as well as any document or item marked as confidential.

I understand that I am prohibited from disclosing any confidential respondent information which has been obtained during the course of a study to anyone other than authorised NatCen staff (or authorised freelancers, sub-contractors or collaborators).

I undertake not to use the information for any purpose other than for the purpose I have specifically been authorised to undertake with NatCen.

I agree to return any documents or items connected with my work with NatCen and shall not retain any copies unless specifically authorised.

I confirm that I have carefully read and understood this agreement.

Organisation name	
Name	
Signature	
Date	