

Safe Share Service Terms and Conditions

Safe Share Service Terms and Conditions

Version 1.3 ? October 2017

Introduction

Safe Share allows the secure exchange of data between Customer Client sites via an encrypted overlay over existing networking infrastructure, for example, over the Janet network, the internet or PSN.

This allows users to have secure remote access to data that they would otherwise have to travel in person to a secure centre to access. Authorised access will be provided either from a secure room or via an approved Customer Client machine depending upon the Information Governance Requirement applicable to the specific Customer.

All use of Safe Share by Customers and their nominated Customer Clients is conditional upon their compliance with these Terms and Conditions, and any additional applicable JSL policies and technical requirements that they may be notified of by JSL from time to time in writing (which may include by email). Furthermore, Customers shall ensure Customer Clients' and End Users' compliance with these Terms and Conditions (to the extent applicable to them).

1. Definitions and Interpretation

Agreement	An order placed [by a Customer and/or Customer Client] for a specified service slice JSL's signed acceptance and these Terms and Conditions.
Customer	The organisation or body authorising Customer Clients to use the Customer's Service Slice(s).
Customer Client	An organisation or individual authorised by a Customer as an entity to connect to Safe Share by means of a Safe Share router or Safe Share VPN client.
End User	A person authorised by a Customer Client or the relevant Management Contact to access data over Safe Share.

Good Practice	Good business practice as generally accepted within the IT industry.
Janet CSIRT	Jisc's Computer Security Incident Response Team handling and managing security incidents on the Janet network.
Jisc	<p>The UK higher, further education and skills sectors' not-for-profit organisation for digital services and solutions. A not-for-profit company limited by guarantee, registered in England.</p> <p>Company name: Jisc</p> <p>Company number : 05747339</p> <p>Charity number: 1149740</p> <p>Vat number : 197 0632 86</p>
Jisc Service Desk	<p>The team responsible for the initial fielding of fault calls or queries for Jisc products and services.</p> <p>Tel: 0300 300 2212</p> <p>07:00 - 00:00 (Monday - Friday)</p>
Jisc Services Limited (JSL)	Company Number 2881024 whose registered office is at One Castlepark, Tower Hill, Bristol, BS2 0JA.
Information Governance Requirement	A defined set of data access processes, governance and security controls required by the Customer and Customer Clients.
Management Contact	An individual notified as such to JSL by the Customer, whose role is to manage the Safe Share service at a Customer Client of the Customer, such management to include the enrolment, provision, and maintenance of service information, and the nomination of other Management Contacts and/or Security Contacts at the Customer Client (as the case may be).
Safe Share	The encrypted overlay network, including hardware, software, configuration and policies required by JSL to provide a higher assured network. This virtual network allows secure data transfer between authorised Customer Clients within a specific Service Slice.

Secure Environment	A location or machine that has the required physical and network security measures in place to comply with the Customer's Information Governance Requirement.
Security Contact	An individual or general-purpose email address nominated by the Customer and/or relevant Management Contact and notified as such to JSL, who/which will receive security-related information, updates or incident advisories on behalf of that Customer or Customer Client (as applicable).
Service Slice	A distinct part of Safe Share dedicated to the Customer Clients of a Customer, which will be designed by JSL, for example in respect of its architecture, to meet the requirements of the applicable Information Governance Requirement. Each Service Slice is independent of each other to prevent communication between Service Slices.

2. General Obligations

1. All Customers and Customer Clients must comply with the applicable policies and technical specifications as notified to them by JSL from time to time.
2. The Customer shall nominate and provide the contact details of at least one person at each Customer Client as its Management Contact and one person or general-purpose email address as its Security Contact. The Customer will maintain an up-to-date list of its Management Contacts and Security Contacts and shall notify JSL if it wishes to make any changes. Any changes with regard to the Customer itself shall be notified to JSL by the Customer directly.
3. The Customer and the Customer Client acknowledges that participating in the Safe Share service does not itself grant it, or the Customer Clients automatic access to the resources of other Safe Share service participants. Such access is conditional upon the Customer or Customer Client agreeing appropriate terms with the relevant Safe Share participants governing that access, and all relevant parties confirming to JSL in writing that they authorise such access. JSL will not be responsible for, nor have any liability in respect of, the performance or otherwise of those terms and will not be required to resolve any disputes in relation to those terms.
4. The Customer and the Customer Client agrees not to act in any manner that damages, is likely to damage or otherwise adversely affect the reputation of JSL, the wider JSL group or the Safe Share service.
5. The Customer and the Customer Client acknowledges that JSL may take any action as is necessary in its opinion to protect the legitimate interests of other Safe Share participants, the reputation of JSL and/or the wider Jisc group, and/or ensure the efficient operation of the Safe Share service. This will be without incurring liability to the Customer and/or Customer Clients, and without prejudice to any other defined rights and remedies.
6. The Customer and/or the Customer Client (as applicable) grants JSL the right to hold, process, publish and use any data necessary for administering and operating the Safe Share service.

7. The Customer and/or the Customer Clients (as applicable) each undertake that:
 1. all and any data when provided by it, their End Users, or any of its representatives (including their Management Contact(s) and Security Contact(s)) to JSL or any other participants in the Safe Share service is accurate and up-to-date;
 2. it will observe Good Practice for the operation of applications and services that use Safe Share including in relation to the configuration, operation and security of its networks and systems (and shall ensure it has the ability to trace activity to an End User account);
 3. it will give all reasonable assistance to JSL and its representatives (including where applicable other Safe Share participants) in any investigation into the misuse of the Safe Share service;
 4. it will promptly inform Janet CSIRT of any apparent breaches of security affecting Safe Share; and
 5. it will provide Secure Environments in accordance with Good Practice for the hosting of Safe Share network equipment and from where End Users can access services via Safe Share.
8. Customers are responsible for the terms of their relationships with Customer Clients. JSL will not be responsible for, nor have any liability in respect of, the performance or otherwise of those terms and will not be required to resolve any disputes in relation to those terms.

3. Customer Client Obligations

1. Customer Clients must agree to these terms and conditions before JSL will supply them with a Safe Share router and/or access to Safe Share.
2. Customer Clients are responsible for ensuring their End Users abide by the **Safe Share Acceptable Use Policy** ^[1] <https://community.jisc.ac.uk/library/network-and-technology-service-docs/safe-share-acceptable-use-policy> ^[2] and the End User section of these Terms and Conditions.
3. Customer Clients will agree a suitable date for installation and testing of the Safe Share routers into their secure environment. The Customer Client shall arrange that its internal support team will be available and access is possible to all required areas prior to the installation date. The Customer Client shall conduct final testing during the installation day.
4. Customer Clients will be required to host the Safe Share router in accordance with the relevant Information Governance Regime, Good Practice, and any instructions provided by JSL in terms of power, physical and environmental security, and to not tamper with or attempt access to the Safe Share router or any other Safe Share equipment provided in any way without JSL's prior written consent.
5. Customer Clients must immediately disable an End User's access credentials at the end of their association with their Customer or Customer Client (as applicable).
6. Customer Client shall ensure that any notification of a fault with the Safe Share router must come from the Customer Client's Management Contact to the JSL Service Desk.
7. It is the Customer Client's responsibility to rule out local connectivity, power or other issues that may be at fault rather than a faulty Safe Share router before contacting the Jisc Service Desk.
8. Each Customer Client must assign the required number of fixed IP addresses from their public IPv4 range and provide these to JSL before the Safe Share routers can be configured and provided to Customer Clients. Customer Clients must allow the

connection from the fixed IP addresses to a JSL-defined range of public IPv4 addresses in Safe Share.

4. End User

1. End Users must abide by the **Safe Share Acceptable Use Policy** [3]

<https://community.jisc.ac.uk/library/network-and-technology-service-docs...> [2]

1. End Users are accountable to, and the responsibility of, the Customer or Customer Client that issues them with their credentials to access services or applications via Safe Share.
2. If an End User believes that their credentials may have been compromised, they must immediately notify their Customer or Customer Client.
3. End Users must abide by the relevant Information Governance Requirement with respect to their use of Safe Share.
4. End Users will not have any direct relationship with JSL over their use of Safe Share. Any issues or problems experienced by End Users with respect to their use of Safe Share must be managed by their Customer Client or Customer.

5. JSL

1. JSL undertakes to protect the security of data travelling between Customer Clients within the relevant Service Slice by implementing Good Practice.
2. Safe Share routers will be commissioned and configured for Customer Clients following written instructions from a Management Contact.
3. JSL will arrange the supply and installation of the Safe Share routers into the Secure Environment/s as per the agreed date.
4. If a Safe Share router develops a fault that cannot be rectified remotely, then JSL will provide a replacement router to the Customer Client within 5 working days. The Customer and/or Customer Client shall be responsible for providing all reasonable assistance requested by JSL, including access (remote or otherwise) to its systems to the extent reasonably necessary.
5. JSL will provide the necessary and appropriate maintenance and configuration management of the Safe Share router deployed at the Customer Client in order to provide the Safe Share service.
6. JSL will not be responsible for any other maintenance, support or operation of the Customer Client's Secure Environment.

6. PSN Service Slice

1. This clause 6 applies where the Service Slice is for PSN services. Capitalised terms that do not appear in the Definitions and Interpretation section of these Terms and Conditions are defined in paragraph A.1 of the PSN Code Template for: Code of Connection, set out at Appendix 1 of these Terms.
2. JSL shall ensure that any PSN and GCN services that it supplies, or are supplied by others, pursuant to this Agreement shall have been awarded and retain at all times a PSN compliance certificate.
3. JSL shall ensure that any PSN and GCN services that it supplies, or are supplied by

others, pursuant to this Agreement are delivered in accordance with the applicable code, codes or Documents of Understanding (DoU).

4. The Customer client shall ensure that any PSN customer environment used to consume PSN and GCN services supplied pursuant to this Agreement shall have been awarded and retain at all times a PSN Compliance Certificate.
5. The Customer Client shall ensure that any PSN customer environment used to consume PSN and GCN services supplied pursuant to this Agreement] shall be provided and maintained in accordance with the applicable code or codes.
6. Each of the parties warrants and undertakes that they shall throughout the term, where specifically requested in writing by the PSN team acting on advice from the Infrastructure SIRO, immediately disconnect its GCN services, PSN services or customer environment (as the case may be) from such PSN services (including any Direct Network Services (DNS)), GCN services and customer environments as the PSN team instructs where there is an event affecting national security, or the security of the GCN or PSN.
7. The parties acknowledge and agree that the PSN team shall not be liable to them or any other party for any claims, proceedings, actions, damages, costs, expenses and any other liabilities of any kind which may arise out of, or in consequence of any notification pursuant to clause 6.6.
8. Each of the parties acknowledges and agrees that these clauses 6.5 and 6.6 are for the benefit of and may be enforced by the PSN team, notwithstanding the fact that the PSN team is not a party to this Agreement, pursuant to the Contracts (Rights of Third Parties) Act 1999.
9. JSL shall cooperate with suppliers of other PSN services and GCN service providers to enable the efficient operation of PSN.
10. The PSN services shall be delivered in a way that enables the sharing of services across customers of PSN services and maximises the savings to be achieved by such sharing of services.

7. Limitation of Liability

1. The Customer must ensure that before any use of the Safe Share service, each of its Customer Clients and their End Users waives any claims of whatever nature, to the extent permitted by applicable law, against JSL or other Customers related in any way to the use of the Safe Share service.
2. The Customer agrees that JSL has no liability whatsoever in respect of errors or faults in the registration or publication of services available via the Safe Share service.

7.3. Nothing in these Terms and Conditions limits or excludes the liability of JSL for death or personal injury caused by its negligence, or for fraud, or any other liability which cannot be excluded or restricted by applicable law.

7.4. JSL provides the Safe Share service on an 'as is' basis, without warranties of any kind, and subject to Clause 7.3, the total liability of JSL, whether in tort (including for negligence or breach of statutory duties), contract, misrepresentation or otherwise, arising under these Terms and Conditions, shall not exceed the total amount paid by the Customer or Customer Client, as applicable, for the Safe Share service in the 12 month period preceding the event giving rise to such a claim.

1. Subject to Clause 7.3 and without prejudice to Clause 7.4, JSL expressly excludes any

liability for loss of profits, loss of business, depletion of goodwill or similar losses, loss of anticipated savings, loss of goods, loss of contracts (whether direct or indirect), loss of use, loss of opportunity, loss, spoiling or corruption of data or information or any special, indirect, consequential or pure economic loss, costs, charges or expenses.

2. The Customer will indemnify, defend, and hold harmless JSL and its affiliates, officers, directors, employees, successors and assigns from and against all claims, suits, demands and actions brought against these indemnified parties, and for all damages, losses, costs, and liabilities in relation thereto, that result or arise from the acts or omissions of the Customer, the Customer Clients and the End Users or otherwise result or arise directly or indirectly from the Customer's, Customer Client's and or End User's access to and/or use of the Safe Share service.
3. Except as expressly provided in these Terms and Conditions, all representations, conditions and warranties in relation to JSL's provision of the Safe Share service, whether express or implied (by statute or otherwise) are excluded to the fullest extent permitted by law.

8. Auditing and Compliance

1. Customers and Customer Clients acknowledge and agree that JSL shall, on reasonable notice, have the right to audit their systems, processes and documentation (either remotely or in person) to verify that they are complying with these Terms and Conditions, any other applicable policies and technical requirements, or general Good Practice in the area of operational security.
2. At least every 12 months Customer will provide to JSL an up to date list of Management Contacts and Security Contacts at each Customer Client.
3. Customers and Customer Clients shall co-operate with and provide such assistance as reasonably required by JSL in connection with such audits.

9. Notification of Non-Compliance and Suspension of Service

1. Without prejudice to JSL's rights under Clause 10, if JSL has reasonable grounds for believing that a Customer or Customer Client is not complying with these Terms and Conditions or any applicable policies and technical requirements, then JSL may:
 1. notify the Customer or Customer Client of such non-compliance in sufficient detail to allow it to take appropriate remedial action;
 2. notify the Customer of such non-compliance by the Customer Client in sufficient detail to allow it to take appropriate remedial action; and
 3. at JSL's discretion, immediately suspend the Customer Client's use of the Safe Share service.

Following receipt of such notice, the Customer must promptly remedy the non-compliance.

1. JSL shall lift the suspension on a Customer Client under Clause 9.1.3 above if the Customer Client remedies the notified non-compliance to the satisfaction of JSL.

10. Termination of Service

1. A Customer or Customer Client may voluntarily terminate its participation in the Safe Share service upon at least one (1) month's written notice to JSL.
2. JSL may terminate the operation of the Safe Share service upon no less than three (3)

months? written notice to Customers and its Customer Clients.

10.3.JSL may immediately terminate the participation of a Customer Client or a Customer in the Safe Share service by giving written notice, without any compensation or damages due to the Customer Client or Customer, but without prejudice to any other rights or remedies which JSL may have, if the Customer Client or Customer:

1. has materially breached these Terms and Conditions or any applicable policies or technical requirements and such breach is incapable of remedy; or
2. has a receiver, administrative receiver, administrator or other similar officer appointed over it or over any part of its undertaking or assets or passes a resolution for winding up (other than for the purpose of a bona fide scheme of solvent amalgamation or reconstruction) or a court of competent jurisdiction makes an order to that effect or if the Customer Client or Customer becomes subject to an administration order or enters into any voluntary arrangement with its creditors or ceases or threatens to cease to carry on business or is unable to pay its debts or is deemed by section 123 of the Insolvency Act 1986 to be unable to pay its debts, or undergoes or is subject to any analogous acts or proceedings under any foreign law, including, but not limited to, bankruptcy proceedings.
3. If JSL has notified a Customer Client or a Customer that it is not complying with these Terms and Conditions or any applicable policies and technical requirements and required it to remedy the same, and the Customer Client or Customer has not remedied the non-compliance to the reasonable satisfaction of JSL within 30 days of the notice, JSL may terminate their use of the Safe Share service.
4. Where a Customer Client or Customer ceases to use or ceases to be entitled to use the Safe Share service for whatever reason:
 1. JSL will remove that Customer or Customer Client access to the Safe Share service. In the event that a Customer's access is removed, the access of all related Customer Clients may be removed by JSL at its discretion;
 2. JSL will inform other Safe Service participants of their removal; and
 3. the Customer concerned will inform its Customer Clients and End Users that it is no longer a Customer to the Safe Share service, and will immediately cease using, and shall return to JSL, any JSL equipment (such as routers).

11.Dispute Resolution

11.1. If any dispute arises between a Customer and JSL with respect to these Terms and Conditions, both parties will refer the dispute to their respective representatives in respect of the Safe Share service, who will promptly discuss the dispute with a view to its resolution.

11.2. If any dispute arises between a Customer Client and JSL with respect to these Terms and Conditions, the Customer Client will refer the dispute to their Customer whose representatives in respect of the Safe Share service, will promptly discuss the dispute with JSL with a view to its resolution.

11.3. If any dispute cannot be resolved in accordance with Clauses 11.1 or 11.2 within ten (10) working days, the matter will be referred for consultation between senior executives of the Customer and JSL. If such senior executives are unable to resolve the matter they will refer the dispute to their respective chief executives.

11.4.If a dispute cannot be resolved in accordance with Clause 11.3 within ten 10 working

days of escalation to such chief executives, the parties may proceed to mediation provided by the Centre for Dispute Resolution (?CEDR?) under its Model Mediation Procedure (or such other body as the Parties may agree). Unless otherwise agreed between the parties, the mediator will be nominated by CEDR. To initiate the mediation the parties will send a joint notice in writing ("ADR notice") to CEDR requesting mediation. The mediation will start not later than thirty (30) days after the date of the ADR notice, or such later date as the mediator is available.

1. If a process for mediation is not agreed in accordance with Clause 11.4 within a period of fifteen (15) working days from a request by either party for mediation or from the discussions between the parties? executive directors, and the dispute remains unresolved, both parties shall be entitled to pursue the matter in law.

12. Data Protection and Privacy

1. The Customer and all Customer Clients must comply with any applicable legislation in relation to data protection and privacy, including the Data Protection Act 1998 (as may be updated, renamed or re-enacted from time to time).
2. In so far as it processes any Personal Data, JSL shall process the Personal Data only in accordance with the Customer and/or Customer Client?s instructions from time to time and shall not process the Personal Data for any purpose other than those expressly authorised by the Customer and/or Customer Client.
3. JSL warrants that, having regard to the state of technological development and the cost of implementing any measures, it will:
4. take appropriate technical and organisational measures against the unauthorised or unlawful processing of Personal Data and against the accidental loss or destruction of, or damage to, Personal Data to ensure a level of security appropriate to:
 1. the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and
 2. the nature of the data to be protected.
5. take reasonable steps to ensure compliance with those measures.
6. In this clause, the following words and expressions shall have the following meanings. ?Personal Data? shall have the meaning set out in section 1 (1) of the Data Protection Act 1998 and ?Processing and process? shall have the meaning set out in section 1(1) of the Data Protection Act 1998.

13. Service Management and Assignment

1. JSL has the right to assign its rights and benefits under these Terms and Conditions. If the management function of the Safe Share service is transferred from JSL to another body, the participation of a Customer or Customer Client will continue unaffected and these Terms and Conditions will be enforceable by such successor body.

14. Updates and Variations

14.1. These Terms and Conditions, and any other policies or technical requirements referred to in these Terms and Conditions may be updated or amended by JSL from time to time. Any such updates or variations shall be notified in writing to Customers and Customer Clients (which may include by email) at least thirty (30) days in advance of the

relevant changes taking effect. If a Customer or Customer Client cannot or is not prepared to accept such changes, it should notify JSL within ten (10) working days of receipt of JSL's notice of such change accordingly and its participation in the Safe Share service shall be treated as terminated from the date on which such change(s) take(s) effect.

15. Governing Law

1. These Terms and Conditions will be governed and construed in accordance with the laws of England and Wales, and JSL, the Customer and Customer Clients irrevocably submit to the exclusive jurisdiction of the Courts of England and Wales.

Appendix 1. Defined terms from PSN standard terms and conditions

Also available at:

<https://www.gov.uk/government/publications/psn-standard-terms-and-conditions/psn-standard-terms-and-conditions> ^[4]

CESG	The UK government's National Technical Authority for Information Assurance. See www.cesg.gov.uk ^[5]
Code of Connection or CoCo	The agreement, as set out in the code template, setting out the obligations and requirements for organisations wanting to connect to the PSN, together with all documents annexed to it and referenced within it.
Code of Interconnection or CoICo	The agreement, as set out in the code template, setting out the obligations and requirements for an organisation to provide PSN connectivity services, together with all documents annexed to it and referenced within it.
Code of Practice or CoP	The agreement, as set out in the code template, setting out the obligations and requirements for an organisation wanting to provide PSN services, together with all documents annexed to it and referenced within it.
GCN Service Provider or GCNSP	A component, product or service that enables PSN-connected organisations to enjoy intra and inter-organisation IP data transmission and for which a PSN compliance certificate has been awarded by the PSN team.
Government Conveyance Network or GCN	The total network of all GCN services provided by all GCN Service Providers.

PSNconnectivity service	A component, product or service that enables PSN-connected organisations to enjoy intra and inter-organisation IP data transmission and for which a PSN compliance certificate has been awarded by the PSN team.
PSNconnectivity service provider	An organisation that is supplying or is approved to supply a PSN connectivity service in accordance with a ColCo.
PSNcompliance certificate	The certificate awarded to the individual infrastructures, GCN Services, PSN services and PSNconnectivity services that make up the PSN.
PSN customer	The PSN service consumer that has achieved PSN compliance certification for their PSN customer environments and holds PSN supply agreement(s) with PSN service providers and PSNconnectivity service providers for the services concerned.
PSN supply agreement	Either a contract or ? if it is between public sector bodies ? a Memorandum of Understanding (MoU) to deliver PSN services or PSN connectivity services.
PSN service consumer	An organisation which uses PSN services or PSN connectivity services.
PSN Service Provider or PSNSP	An organisation that is supplying or is approved to supply PSN services in accordance with a CoP.
PSN service	A functional service available to PSN-connected organisations from a PSN-connected infrastructure in order to enable the fulfillment of a specific business activity, which is offered by a PSN Service Provider in accordance with a CoP and for which a PSN Compliance Certification has been awarded by the Public Services Network Team.
Public Services Network or PSN	The government?s high-performance network, which helps public sector organisations work together, reduce duplication and share resources.

Source URL: <https://community.jisc.ac.uk/library/network-and-technology-service-docs/safe-share-service-terms-and-conditions>

Links

[1]

[https://corp.jisc.ac.uk/filestore/LumenHouse/Projects/The%20safe%20share%20project/Project%20Plan/Transition%](https://corp.jisc.ac.uk/filestore/LumenHouse/Projects/The%20safe%20share%20project/Project%20Plan/Transition%20Plan)

[2] [https://community.jisc.ac.uk/library/network-and-technology-service-docs/safe-share-acceptable-use-](https://community.jisc.ac.uk/library/network-and-technology-service-docs/safe-share-acceptable-use)

