Building human networks to drive forward innovations in international data access: Introducing the International Secure Data Facility Professionals Network (ISDFPN)

Deborah Wiltshire[1], Beate Lichtwardt[2], and Libby Bishop[3]

Abstract

The International Secure Data Facility Professionals Network (ISDFPN) was set up in 2022 as part of the Social Sciences and Humanities Open Cloud project (SSHOC) to bring together international colleagues working in or towards Trusted Research Environments (TREs), to share expertise and experiences, and to spark collaboration as well as develop new ideas.

While various international networks and collaborations exist currently, these aim to improve the international data infrastructure landscape, and mainly focus on establishing connections between TREs. However, there is also a forum needed for those working in these TREs, which provides a platform for regular knowledge exchange as well as opportunities to drive innovation. ISDFPN is not a network for developing infrastructure, rather it is a place to share experience, expertise, and ideas, which is not yet formally available internationally. As the fast-changing secure data landscape evolves, this Network will be a vital resource for collaborative work towards finding solutions for shared and emerging problems experienced by TRE staff. Where TREs are at different stages in their development, such a forum is vital as services seek to learn from each other.

The ISDFPN held its first virtual meeting on 30 March 2022, and, although the SSHOC project ended in April 2022, the group has continued to meet twice a year, co-Chaired by the UK Data Service, and GESIS Leibniz Institute for the Social Sciences. This paper traces the ISDFPN from its origins and highlights both its aims and objectives as well as its activities so far.

Keywords

Trusted Research Environments, TREs, secure data facilities, international data access, secure access data, secure data, controlled data, professional networks

Introduction

Enabling safe, efficient, and impactful research on societal challenges is crucial to facilitate evidence-based policy development and effecting positive change for daily lives and livelihoods within and across countries. In order to provide the foundation for such essential research, increasingly more Trusted Research Environments (TREs) are enabling access to very detailed, sensitive microdata.[4]

It was the National Statistical Institutes (NSIs) that took the lead in the early 2000s in setting up physical Safe Rooms to provide on-site access for researchers to their sensitive, potentially disclosive microdata. In the years that followed other entities followed suit in establishing Safe Rooms for on-site access to sensitive data, including several national data archives such as the UK Data Archive and

Microdata Online Access (MONA) – Statistics Sweden, and research institutes such as the Leibniz Institute for Educational Trajectories (LifBi). On-site access has several disadvantages for researchers though, e.g. the expense of traveling to sometimes quite distant physical locations and the associated time constraints of short research visits (Bishop et al, 2022).

By 2011, work was well underway to move towards offering remote access to microdata, either via remote desktop systems (e.g. UK Data Archive) or via remote job execution (e.g. Institute for Labor Market and Occupational Research of the Federal Employment Agency - Research Data Center (IAB-FDZ)). Starting in 2013, the UK Data Archive has successfully enabled remote desktop access to its controlled (secure access) data via the UKDS SecureLab, playing a longstanding part in the UK data provision landscape. This service broke new ground by removing the need to travel to a fixed location for accessing detailed microdata, and 'secure remote access to data in the UK was born' (Welpton, 2021; Scott, Lichtwardt & Woods, 2022). UKDS SecureLab, initially called the Secure Data Service (SDS), was the first national Secure Data Facility in the UK providing accredited researchers with secure remote access to controlled data, including a wealth of linked longitudinal datasets. Following the UKDS SecureLab provision and best practice, other TREs in the UK – for instance, the Office for National Statistics' (ONS) Secure Research Service (SRS) – moved towards offering remote access. UKDS SecureLab has therefore 'provided the blueprint' (Welpton, 2021) for secure remote data provision in the UK and beyond.

In Germany, selected Research Data Centres (RDCs) also enable remote access. For example, the Research Data Center at the Leibniz Institute for Educational Trajectories (LIfBi) prepares and disseminates survey data from the German National Educational Panel Study. More sensitive versions of the data are made available via their remote desktop system 'RemoteNEPS', whilst the most sensitive data remains accessible only via their Onsite Data Security room in Bamberg. GESIS Leibniz Institute for the Social Sciences has provided access to sensitive data via its Secure Data Center Safe Room, a physical data enclave, since 2013. In 2020, a new programme of work began to develop a new remote desktop access system. This will remove the need for researchers to travel, often some distance, to the Safe Room to access these data.

It has long been recognised that enabling cross-border international access to sensitive data would be a positive move forwards in the international data access landscape and already in the 2000s there were a few initiatives to enable Safe Room Remote Desktop Access across international borders (Bishop et al, 2022; Woollard et al, 2021). The Holy Grail was to find ways to enable researchers to visit a Safe Room in one country to remotely access sensitive data held by a TRE in another country.

A recent review of the secure data access landscape showed that progress in this area was initially quite slow (Bishop, 2021), but one of the early success stories was the 2004 opening of an access point at the Inter-university Consortium for Political and Social Research (ICPSR) in the US to the IAB-FDZ in Germany and the subsequent opening of access points in numerous Safe Room locations at TREs both within Germany and internationally[5]. In 2018, the International Data Access Network (IDAN) was founded[6] as a collaboration between six European Research Data Centres, including CASD (France), CBS (The Netherlands), GESIS (Germany), IAB (Germany), the UK Data Service (UK), and ONS (UK), forming a network to facilitate research use of secure access data via reciprocal provision of Safe Room Remote Desktop Access. The most recent development was the setting up of a bilateral remote access connection between the UKDS SecureLab and the Secure Data Center at GESIS, Cologne as part of the Social Sciences and Humanities Open Cloud (SSHOC) project, a large EU collaboration of 47 organisations[7] (Wiltshire, Voronin & Lichtwardt, 2022; Lichtwardt et al, 2022; Lichtwardt & Wiltshire, 2023). This marked a significant step forward in the drive towards opening international access to sensitive data.

Due to limited funding, legal barriers and other challenges, most of the infrastructure development for remote access has thus far occurred in a bottom-up fashion, mostly on an individual institutional level or else with small-scale bilateral collaborations. Too often NSIs have little incentive to invest in such collaborative infrastructure as this is usually not in their mandates, and national data archives generally have other priorities and limited resources to invest in the development of international data access infrastructure. Nonetheless, there is a growing list of Secure Data Facilities and corresponding demand from researchers, driving improvements.

Infrastructures must, of course, provide essential 'plumbing' - hardware, software, platforms, resources, and so on. However, without adequate human support such as a full complement of staff, skills, training, etc., too often infrastructures are built but not adopted, embraced but not established, or started but not sustained. By nature of their specialist niche, TRE staff tend to be widely distributed, sometimes it is only a single individual within a large institution. Therefore, improving the human network landscape, especially internationally, is essential. Even for well-established national TREs, a substantial amount of work and expertise is required to enable Safe Room Remote Desktop Access across borders.

With the now rapidly evolving international secure access data landscape, professionals working in TREs need a more structured mechanism for exchanging knowledge, learning from each other, as well as having access to and contributing to a one stop shop for relevant materials and resources (resource platform). Within the TRE sector, dedicated, experienced staff grapple with the challenges of facilitating access to and keeping safe a growing range of sensitive and potentially disclosive data, even more so with newly emerging challenges of new international sensitive data access possibilities. This work comes with a unique set of tasks that must be conducted within an often-complex legal governance landscape. It has long been recognised within the sector that little formal training or support is available to provide guidance and assistance for these roles. For new TRE staff, training is primarily 'on the job' with support provided only by their colleagues. This approach can work in larger TREs where new recruits have access to more experienced colleagues but falls short in smaller TREs where there may be just one or two full-term team members. It also falls short in helping TRE staff develop their skills and advance their careers. As the number of TREs, and consequently the number of those working in TRE settings, grew, a move started to change this 'on the job' approach to active support, with the belief that providing more substantial and sustained human support would also do a great deal to advance and support the developments of national as well as international secure data access.

The SDAP group - an example of a national Safe Data Access Professionals network

There are several examples of national safe data access professional networks both nationally and interationally (across Europe and beyond). RDC-Net, for example, aims to bring together participating TRE partners from across Germany[8]. Multi-nation projects such as IDAN and SSHOC bring together the international community. However, their primary focus lies on practical outcomes such as developing infrastructure or establishing cross-organisational connections rather than on providing support and development for the practitioners.

In the UK, a long-established network, the Safe Data Access Professionals (SDAP) group which started as an informal gathering in 2011, provides training and support via a Forum for data stewards working in TREs across the UK[9]. Early members came primarily from the consortium of organisations tasked with making Office for National Statistics data and ESRC-funded Longitudinal Studies data available. The group's original aim was to support professionals working within this very specialised sector. Throughout the evolution of the group, it has become more formalised, and its membership has grown substantially but its primary aim remains professionalising the work of data stewards working in TREs and giving them a forum where they can exchange experiences and expertise with peers from across the sector. The group currently has around 50 members from across the UK. The group meets quarterly, with all activities and future planning being overseen by a steering committee. Participation in this group has brought many benefits to its members, not least in providing a forum where they can talk about their work and where they can seek expert advice from others familiar with the regulatory landscape within which they work.

The SDAP group not only provides vital support to TRE data stewards, but through its members it has produced several important deliverables focused in three main areas: researcher training, staff skills and competencies, and Statistical Disclosure Control (SDC), that are widely utilised across the sector.

1. Researcher training: In the UK it is often a mandatory requirement for researchers to receive some form of training prior to gaining approval to access secure data. Even where this is not mandatory, many TREs are now looking at developing their own researcher training. SDAP members from Cancer Research UK and The Health Foundation developed a set of canonical training materials that can be freely downloaded and adapted by other services as needed[10]. This approach was adopted later by the SSHOC project team who developed a new canonical set of training materials for the European TRE sector (Wiltshire, 2021; Wiltshire, 2024).
2. Staff skills and competencies: The area of staff skills and development is perceived as an important area to address as staff often come into the sector more by accident than design, and whilst they gain considerable skills through their work, the role of the secure data steward has not been professionalised. Since 2016, the SDAP group have been working to develop a Competency Framework[11]. The Competency Framework sets out the skills required for staff working in Secure Data Facilities and can aid staff development as a way of setting objectives, identifying strengths and areas for improvement, performance management, and preparing for future roles within the sector. It also designed to assist TREs with the process of recruiting new staff.
3. Statistical disclosure control: In 2017, the SDAP group began reviewing the available guidance on Statistical Disclosure Control. The review concluded that the existing guides were by then some years old, and whilst the primary theoretical principles of SDC have changed little, new methodologies and data types had emerged. The result of this review was the publication by the SDAP group of the SDC Handbook in 2019, followed by its translation into Spanish in 2020[12]. The SDC Handbook was widely applauded and is considered the main ‘go to’ guide for TRE data stewards responsible for carrying out statistical disclosure control.

The SDAP group have their own website where these resources and others including presentation slides from previous meetings and events are made freely available to anyone interested in TREs and sensitive data access and use[13].

The International Secure Data Facility Professionals Network (ISDFPN)

With the expansion of secure data access possibilities across international borders via projects and collaborations such as IDAN and SSHOC, it was recognised that a network would be highly beneficial to those tasked with developing and running these internationally focused TREs. Secure Data Facility professionals working within these services are stepping into new, uncharted territory and as such, there is an emerging need to provide a space for secure data professionals internationally to meet one another, to exchange knowledge, and discuss pertinent issues arising from these new connections. Until 2022 there was no formal intenational forum for secure data professionals that allowed sharing of experiences and expertise. Similar to the the UK, there was no clear career path to train data stewards to work in TREs. As more international bilateral connections are built, the establishment of an international forum became an urgent priority.

The International Secure Data Facility Professionals Network (ISDFPN) was set up in 2022 as part of the Social Sciences and Humanities Open Cloud project (SSHOC) with the aim of bringing together international colleagues working in or towards Trusted Research Environments (TREs) and to provide support and collaborative opportunities to the international TRE community (Lichtwardt, Wiltshire & Bishop, 2022). The Network is open to different disciplines including the social sciences, the health sector and humanities. ISDFPN is unique in discussing issues not only in relation to quantitative secure data but also actively working on, for the first time, generating options for making qualitative sensitive data available in via Secure Data Facilities in the future.

The ISDFPN group started as a formal structure. The International Secure Data Facility Professionals Network (ISDFPN) was set up as part of the Social Sciences and Humanities Open Cloud (SSHOC) project, which ran from January 2019 until April 2022. The UK Data Service has been leading the SSHOC deliverable to setup and establish this Network as a member of Work Package 5 ('Innovations in Data Access'), Task 5.4 'Remote Access to Sensitive Data'. Since the conclusion of the SSHOC project, the Network is stewarded through a collaboration between the UK Data Service (UKDS Secure Lab) and GESIS Leibniz Institute for the Social Sciences (Secure Data Centre). Prior to the first ISDFPN meeting Terms of Reference (ToR) were drafted so they are ready for discussion and comments during the first meeting[14]. The timing and frequency of meetings (Steering Group Meetings, topical Member Meetings) were outlined in the ToR, and the chair and secretariat were named. The ToR also outlines the objectives and deliverables of the group, which are illustrated below.

Table 1 Objectives and Aims of the ISDFPN

Objectives	**Deliverables**
Set the strategic direction for the ISDFPN	Establish a Steering Group for ISDFPN
Oversee the achievement of deliverables	Agree on an annual calendar of meetings and events for ISDFPN members and the wider TRE community
Establish ISDFPN as an ongoing forum within an international context	Identify strategic needs and set up work streams with associated projects[15]
Run topic-based networking and knowledge exchange events for both ISDFPN members and the wider TRE community	Agree and oversee the communications and digital strategy
Ensure collaboration with other professional groups where appropriate	Agree on a basic action plan (annual planner including all meetings, events, and work strands)

Foster continued collaboration amongst ISDFPN members and the wider TRE community	Develop a Community Code of Conduct for ISDFPN members and for all external public facing forums e.g., events, social media platforms

Further work streams will be established as the group evolves and grows. Key goals and deliverables may also change from year to year in response to changes in the international secure data access landscape.

Meetings are held bi-annually, and, for reasons of inclusivity, online. There are two presentations at each meeting, exploring and discussing issues related to quantitative and qualitative secure data. The ISDFPN group held its inaugural meeting on 30 March 2022. The meeting was attended by twenty-two people from 13 different institutions, and 5 countries. A number of other people expressed interest in joining the Network, even though they were unable to join the first meeting.

The Inaugural ISDFPN Meeting

In the inaugural meeting attendees were asked to brainstorm ideas about current and future staff skills and staff training needs in TREs.

The following four staff skills and training questions had been placed in a collaborative document:

- Are there skills missing at this point in time?
- What training is needed? Does this exist, and, if so, where?
- What skills might the TRE professional of 2032 need?
- Other thoughts/comments?

Missing skills at this current time identified by participants included machine learning and AI; statistical software programming; anonymisation and pseudonymisation tools; synthetic data techniques; talking to data holders; workflows for ingesting data; research reproducibility; and knowledge regarding non-tabular data. When asked to look into the future and anticipate what skills the TRE professional of 2032 might need, participants listed confidence, awareness of ethical complexities in outputs, and automation of low-level outputs as key priorities.

In terms of training needs, the group acknowledged that some training resources exist already such as the Output Checker Course offered by the DRAGon project, the Safe Researcher Training (SRT) provided by many UK TREs, and FAIR data stewardship training. In addition, many data archives run annual Summer Schools which include courses on research data management. But it was felt that an overview of which TREs offered remote access to sensitive data sources and of what training was currently on offer would be a useful exercise, and that certificates or other formal recognition for training participation would be an important step forward. Having a system for formal recording or recognising training activities led to an expressed desire to see the status and pay of staff involved in key TRE tasks such as Statistical Disclosure Control (SDC) increase, and the lack of role professionalisation tackled, especially given the major legal implications of these tasks. Further comments suggested a diversification of roles might be required within TREs to reflect the increasing complexity of services involved.

The second brainstorming exercise focused on gathering future topics that would be relevant to and of interest to the group as a precursor towards identifying possible work strands for the first few years of the Network and towards building a calendar of topics for the Network meetings. This sparked a lively and engaged conversation with a long wishlist of topics that included among other things:

- An overview of existing TREs/TRE Infrastructure, including provision of remote access systems
- An overview services involved in ISDFPN and future directions
- Technical infrastructures for secure data
- Automatization of Secure Data Facility tasks (e.g., output checking; self-administration platforms for users)
- Public Engagement and involvement
- Legal challenges such as how GDPR supports remote secure data access
- Authentication and authorisation procedures
- Qualitative data in Secure Data Facilities
- Resources library or Knowledge bank.

Whilst the list gave the Network plenty to work with, it was clear from the discussions that the group wished to start with an inventory of what is available at present, and further discussions about what direction the group should take. This starting point was followed closely, according to the group, by topics where there is a need for consensus on best practice, such as technical infrastructure and solutions, legal questions and solutions to manage and scale up the daily workloads.

Events so far

Since the first meeting in March 2022, and after the end of SSHOC, we had three more meetings/events all of which sparked great interest and very fruitful discussions. The topics presented in each of the meetings are detailed in the table below.

Table 2 ISDFPN Meetings - Themes and Dates

Meeting	Date	Presentation 1	Presentation 2
1	30.03.2022	International Secure Data Facility Professionals Network (ISDFPN)	Mind the Skills Gap: creating capacity for data access: Compentancy framework
2	07.09.2022	Certifiying reproducibility with confidential data: forst results from the French cascad/CASD cooperation	Data Sharing with RDC Qualiservice
3	08.03.2023	Enabling access to cenfidential qualitative data through data enclaves	Building a Safe Researcher Accrediatation Scheme
4	06.09.2023	Researcher Passport: A digital user credential for assessing restricted data	Introducing the Safe Points
5	17.04.2024	SANE: an off-the-shelve, data holder-agnostic TRE	Output Disclosure Control for Qualitative Data in Trusted Research Environments: Current State and Next Steps

All of the topics are along the themes that attendees have mentioned in the initial brainstorming exercises. The presentations and discussions have been proven to be extremely valuable and have already led to new connections being made.

Meanwhile, in our fourth meeting, we have repeated the second part of our initial exercise and asked members to identify three topics that they would like to see covered in our ISDFPN Meetings in 2024. This way we ensure we know what the expectations of the group are, and are able to look for inspiration on these topics worldwide. Equally, we are looking for new developments to share with the group, e.g., the development of the SafePod Network[16] to offer also SafePoints, a portable TRE infrastructure system that could be shipped and installed anywhere in the world. We are evaluating what that could mean for the international community and trying to develp standards for adoption of technical solutions, enabling remote access much quicker, at a higher-standard.

Outlook

The international TRE community's response to the first and all subsequent ISDFPN meetings clearly demonstrates the need and desire for such a network. Whilst the SSHOC project was the original driver for setting up the Network, the Network has continued following the official end of SSHOC in April 2022, under the joint stewardship of the UK Data Service and GESIS-Leibniz Institute for the Social Sciences. The first deliverable, to appoint a Steering Group, has been completed and the group now meets bianually to drive the Network forward and to oversee work on the remaining deliverables. Steering Group members come from across the two lead organisations and contribute their time on a voluntary basis. Post-SSHOC the Network received no formal funding, so the secretariat has been provided from existing resources at the UK Data Service. A new EU funded project, EOSC-ENTRUST[17], aimed at creating a European network of trusted research environments, will now provide support for the Network until early 2027. This support will hopefully enable the Network to increase the regularity of its meetings to 3-4 times per year, and to consider having a dedicated website.

Since its inaugural meeting in March 2022, the Network has held whole group meetings twice a year, with two guest presentations each time covering topics such as proposals for a safe researcher accreditation system in Germany, qualitative secure data sharing explorations , enabling reproducibility of findings based on secure access data, and other new developments such as the opportunities a Safe Researcher Passport type scheme currently being proposed in several countries could offer[18]. Whilst the Network is still in its infancy, it has made a strong start in building constructive and collaborative connections across the global TRE community that are vital for advancing work to facilitate international access to sensitive data. Projects like IDAN and SSHOC have highlighted the importance of having consensus over minimum requirements, comparable standards and procedures across TREs for agreeing and implementing bilateral data access solutions. Whilst IDAN, EOSC-ENTRUST and other projects focus on infrastructure development and setting up connections, ISDFPN will play a key role by providing a forum where discussions can occur, TREs can share and exchange knowledge and drive new developments, such as qualitative data in Secure Data Environments, while bridging the gap between different disciplines.

The ISDFPN chairs have been active in promoting the Network through presentations at international conferences and through other networking activities and these activities play a key role in recruiting new members globally. Membership in the Network continues to grow; as of January 2024 it had 33 individual members from 25 organisations across 9 countries[19]. The Network's communication is managed via a dedicated JISC mailing list. ISDFPN welcomes new members. Joining is free, and open to all those who are involved in Safe Data Facilities around the world.

References

Bishop, L. (2021). ’MS28 Assessment of Existing Platforms (1.0)’. *Zenodo.* https://doi.org/10.5281/zenodo.5914390 (Accessed 28/07/2023).

Bishop, L., Broeder, D., van den Heuvel, D., Kleiner B., Lichtwardt, B., Wiltshire, D. & Voronin, Y. (2022). ’D5.10 White Paper on Remote Access to Sensitive Data in the Social Sciences and Humanities: 2021 and beyond (1.0)’. *Zenodo.* https://doi.org/10.5281/zenodo.6719121 (Accessed 28/07/2023).

International Data Access Network (2023) *IDAN – International Data Access Network*. Available at: https://idan.network/ (Accessed 29/09/2023).

Lichtwardt, B and Wiltshire, D. (2023). ’Crossing borders without leaving – sharing secure data internationally’. *UKDS Data Impact blog,* 20 June 2023. https://blog.ukdataservice.ac.uk/sharing-secure-data/ (Accessed 28/09/2023).

Lichtwardt, B., Wiltshire, D. and Bishop, L. (2022) ‘D5.12 International Secure Data Facility Professionals Network (ISDFPN)’. *Zenodo*. https://doi.org/10.5281/zenodo.6583379 (Accessed 03/07/2023).

Lichtwardt, B., Woollard, M., Wiltshire, D. & Bishop, L. (2022). D5.11 ERAN Pilot: Setting up a Secure Remote Connection between two Trusted Research Environments (1,0). *Zenodo.* https://doi.org/10.5281/zenodo.6676393 (Accessed 15/08/2023).

KonsortSWD (2023) *Secure data access point network – RDCnet*. Available at: RDCNet https://www.konsortswd.de/en/konsortswd/the-consortium/services/rdcnet/ (Accessed 29/09/2023).

Scott, J., Lichtwardt, B. and Woods, C. (2022) ’UK Data Service SecureLab: pioneers in enabling safe data-driven research for over a decade’ *UKDS Data Impact blog,* 12 January 2022. Available at: https://blog.ukdataservice.ac.uk/securelab-ten-year-anniversary/ (Accessed 03/09/2023).

Scott, J and Woods, C. (2020) ’Statistical Disclosure Control Handbook now available in Spanish. UKDS Data Impact blog.’ *UKDS Data Impact blog*, 23 July 2020. Available at: https://blog.ukdataservice.ac.uk/statistical-disclosure-control-handbook-spanish/ (Accessed 05/04/2022).

Safe Data Access Professionals (2023) *Safe Data Access Professionals: Home.* Available at: https://securedatagroup.org/ (Accessed 29/09/2023).

Welpton, R. (2021) ’Celebrating 10 years of secure remote access in the UK’. *UKDS Data Impact blog,* 12 October 2021. Available at: https://blog.ukdataservice.ac.uk/ten-years-secure-remote-access/ (Accessed 29/09/2023).

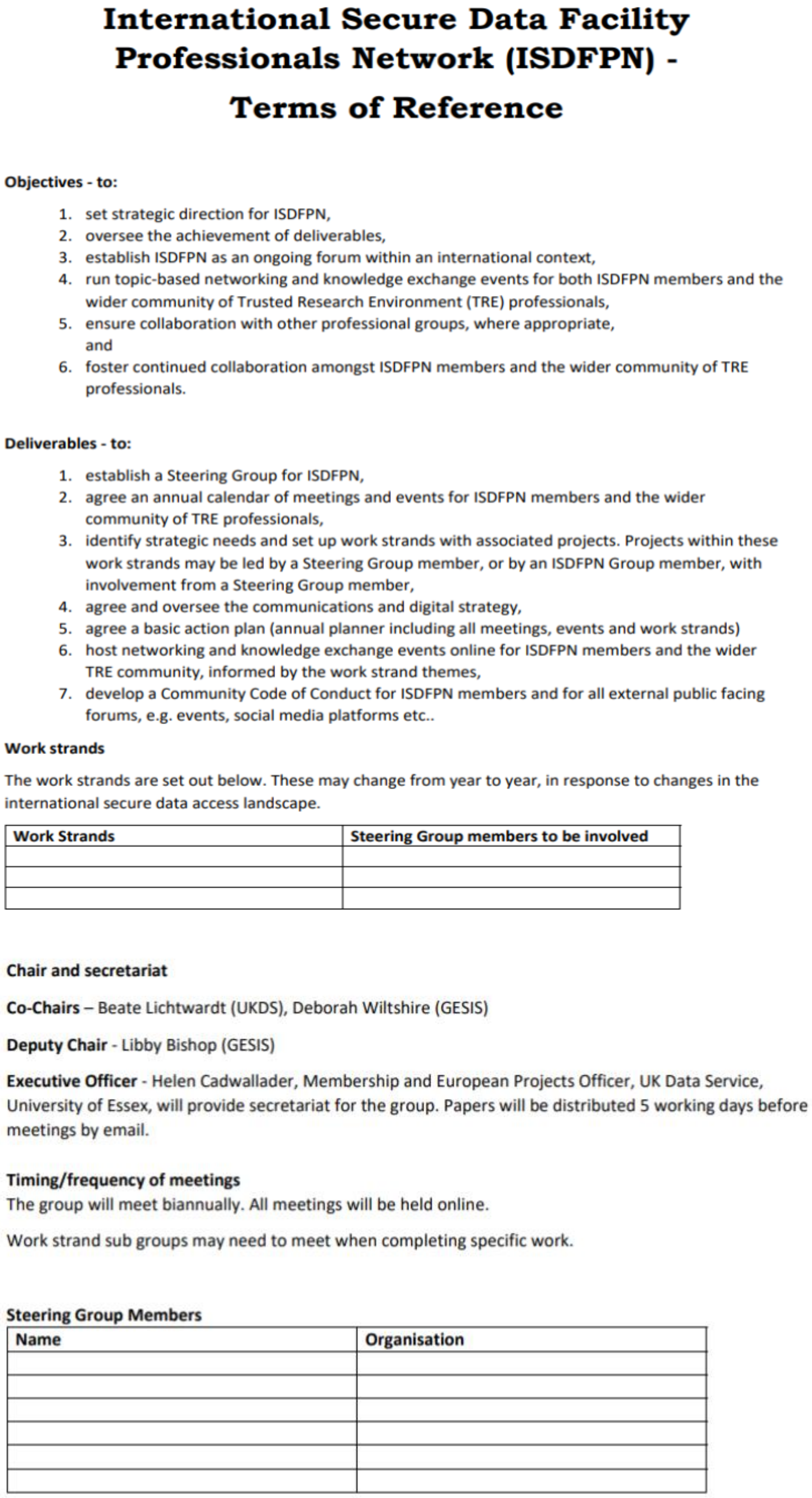
Wiltshire, D. (2021) ’D5.20 Training materials of workshop for secure data facility professionals (v1.0)’. *Zenodo*. https://doi.org/10.5281/zenodo.5638596 (Accessed 03/07/2023).

Wiltshire, D. (2024). Developing canonical ‘safe researcher’ training materials for trusted research environments. IASSIST Quarterly 48 (1). https://doi.org/10.29173/iq1093/.

Wiltshire, D, Voronin, Y. and Lichtwardt, B (2022) ‘M29 Tested connections between partners with live data and researcher projects (V1.0)’. *Zenodo.* https://zenodo.org/record/7684215#.Y_3pNXbMJPZ (Accessed 03/07/2023).

Woollard, M., Lichtwardt, B,. Bishop, L and Müller, D. (2021) ’D5.9 Framework and contract for international data use agreements on remote access to confidential data (v1.0)’. *Zenodo.* https://doi.org/10.5281/zenodo.4534286 (Accessed 03/07/2023).

Appendix 1: ISDFPN Terms of Reference



International Secure Data Facility Professionals Network (ISDFPN) - Terms of Reference

Objectives - to:

1. set strategic direction for ISDFPN,
2. oversee the achievement of deliverables,
3. establish ISDFPN as an ongoing forum within an international context,
4. run topic-based networking and knowledge exchange events for both ISDFPN members and the wider community of Trusted Research Environment (TRE) professionals,
5. ensure collaboration with other professional groups, where appropriate, and
6. foster continued collaboration amongst ISDFPN members and the wider community of TRE professionals.

Deliverables - to:

1. establish a Steering Group for ISDFPN,
2. agree an annual calendar of meetings and events for ISDFPN members and the wider community of TRE professionals,
3. identify strategic needs and set up work strands with associated projects. Projects within these work strands may be led by a Steering Group member, or by an ISDFPN Group member, with involvement from a Steering Group member,
4. agree and oversee the communications and digital strategy,
5. agree a basic action plan (annual planner including all meetings, events and work strands)
6. host networking and knowledge exchange events online for ISDFPN members and the wider TRE community, informed by the work strand themes,
7. develop a Community Code of Conduct for ISDFPN members and for all external public facing forums, e.g. events, social media platforms etc..

Work strands

The work strands are set out below. These may change from year to year, in response to changes in the international secure data access landscape.

Work Strands	Steering Group members to be involved

Chair and secretariat

Co-Chairs – Beate Lichtwardt (UKDS), Deborah Wiltshire (GESIS)

Deputy Chair - Libby Bishop (GESIS)

Executive Officer - Helen Cadwallader, Membership and European Projects Officer, UK Data Service, University of Essex, will provide secretariat for the group. Papers will be distributed 5 working days before meetings by email.

Timing/frequency of meetings

The group will meet biannually. All meetings will be held online.

Work strand sub groups may need to meet when completing specific work.

Steering Group Members

Name	Organisation

[1] Deborah Wiltshire (Corresponding author); GESIS-Leibniz Institute for the Social Sciences, Unter Sachsenhausen 6, 50667 Cologne, Germany; deborah.wiltshire@gesis.org; Orcid 0000-0001-6533-2426.

[2] Beate Lichtwardt; UK Data Service, University of Essex, Wivenhoe Park, Colchester, Essex, CO4 3SQ, United Kingdom; blicht@essex.ac.uk; Orcid 0009-0006-5304-5634.

[3] Libby Bishop; GESIS-Leibniz Institute for the Social Sciences, Unter Sachsenhausen 6, 50667 Cologne, Germany; elizabethlea.bishop@gesis.org

[4] Increasingly, personal/confidential, and sensitive data are made available through Secure Data Facilities which can be also referred to as Secure Access Facilities/ Secure Research Facilities/ Safe Settings/ or Trusted Research Environments (TREs). Examples for these are a) Research Data Centres (RDCs), e.g., the IAB FDZ, RDC LIfBi, RDC SOEP, b) Datalabs, such as the UKDS SecureLab, HMRC Datalab, ONS SRS, Justice Data Lab etc., and c) Data Safe Havens, to name just a few.

[5] https://fdz.iab.de/en/about-us/appointment-locations-and-fdz-online-calendar/ [Accessed 05/04/2022]

[6] https://idan.network [Accessed 05/04/2022]

[7] https://sshopencloud.eu [Accessed 08/04/2024]

[8] https://www.konsortswd.de/en/konsortswd/the-consortium/services/rdcnet/ [Accessed 05/04/2022]

[9] https://securedatagroup.org/ [Accessed 03.08.2023]

[10] https://securedatagroup.org/training2/ [Accessed 05/04/2022]

[11] https://securedatagroup.files.wordpress.com/2018/07/sdap_competency_framework-01_00.pdf Accessed 05/04/2022]

[12] https://securedatagroup.org/sdc-handbook . Some of the authors discussed the reception of the SDC Handbook in this blog published on the UKDS website. Scott, J and Woods, C. (2020) 'Statistical Disclosure Control Handbook now available in Spanish. UKDS Data Impact blog.' UKDS Data Impact blog, 23 July 2020. Available at: https://blog.ukdataservice.ac.uk/statistical-disclosure-control-handbook-spanish/ (Accessed 05/04/2022).

[13] https://securedatagroup.org/events/ [Accessed 05/04/2022]

[14] Please see Appendix 1 for the complete TOR draft.

[15] Projects within these work strands may be led by a Steering Group member, or by an ISDFPN Group member, with involvement from a Steering Group member.

[16] https://safepodnetwork.ac.uk/ provides portable safe settings for secure data access across the UK [Accessed 08/04/2024]

[17] Home | European network of trusted research environments (EOSC-ENTRUST) project [Accessed 10/04/2024]

[18] A Safe Researcher Passport scheme would provide an electronic record of a researchers affliation and training status that could be used by TREs and data access organisations to carry out authenication and authorisation checks. One example is the ICPSR Researcher Passport: https://radius.icpsr.umich.edu/radius/passport/static/about [Accessed 08/04/2024].

[19] If you would like to join the Network, offer a talk or request more information regarding the Network, please email isdfpn@ukdataservice.ac.uk.