How do researchers understand “Trusted Research”?

Findings of a SPRITE+ Workshop held March 2021

This workshop was organised by SPRITE+, the UK NetworkPlus for Security, Privacy, Identity and Trust in the Digital Economy. SPRITE+ is funded until 31 August 2023 by the Engineering and Physical Science Research Council as part of its Digital Economy programme (grant reference EP/S035869/1). This workshop was part-funded by the Office of the Chief Scientific Advisor for National Security. However, the views expressed in this report are those of SPRITE+ and the workshop participants and should not be taken as an expression of government policy or intention.
Contents

Executive summary.......................................................................................................................... 1
  Summary of breakout discussions................................................................................................. 1
  Concluding remarks....................................................................................................................... 2

How do researchers understand “Trusted Research”? Workshop Findings.................................. 3
  Introduction: The Trusted Research Context ............................................................................. 3
  The workshop............................................................................................................................... 5
  Summary of breakout discussions............................................................................................... 5
  Key areas of risk and concern...................................................................................................... 5
  How can guidance and advice to researchers be improved?......................................................... 6
  What could institutions do to manage risks and help individual researchers?............................ 7
  Concluding remarks..................................................................................................................... 8

Appendix 1: Detailed feedback from breakout discussions.......................................................... 10
  Protecting reputation and values................................................................................................. 10
  Well-being, safety and security of people and partners............................................................... 11
  Cyber security.............................................................................................................................. 12
  Research integrity......................................................................................................................... 14
  Regulatory compliance.................................................................................................................. 15

Appendix 2: SPRITE+, the UK Security, Privacy, Identity, and Trust Engagement NetworkPlus...... 17
  Activities....................................................................................................................................... 17
  Leadership and funding................................................................................................................ 18
Executive summary

SPRITE+ held a workshop in March 2021 to identify ways to improve researcher awareness of issues related to “Trusted Research”, an umbrella term that includes issues related to:

- Regulatory compliance (e.g., Export Controls, the Academic TA Scheme, GDPR, partner-country regulations)
- Protecting IP (including cyber security and data protection issues)
- Conflicts of interest with other research partners
- Risk of foreign interference in research/teaching and academic freedom
- Protecting staff and students overseas
- Reputational risk and ethical issues (including potential misuse/abuse/dual use of research knowledge)

At a strategic level, the government and Universities UK have issued guidance aimed at senior leaders in the Higher Education sector, and many UK universities are actively working on adapting and rolling out the guidance. Although there is government guidance for Principal Investigators (PIs) and research teams, awareness and uptake of this guidance is patchy.

The workshop explored the implications of current guidance for ‘coal face’ PIs and their teams, examining the barriers to awareness and implementation, and suggesting ways to improve the situation. 37 researchers from a range of career stages and research disciplines participated in a series of breakout discussions over three hours.

Summary of breakout discussions

Key areas of risk and concern

1. Participants reported little awareness of the guidance available to help researchers protect their work. This extended to concerns over the roles of individual researchers and their institutions in ensuring appropriate due diligence. Participants were unaware of any UKRI guidance.

2. Participants perceived an inconsistent approach to dealing with Trusted Research issues across different universities, and between universities, government, and industry. Differences in approach for different disciplines were reported; as interdisciplinary research grows, the scope of what needs to be protected is also potentially growing.

3. Participants reported increasing pressure to engage in international collaborations but noted that this would increase the need for due diligence procedures. This could be problematic for researchers as they can: (1) slow the pace of research, which can lead to the loss of collaborators and reputational risk; and (2) be administratively burdensome.

4. Participants raised concerns about potential limitations on academic freedom and the ability of researchers to explore and innovate, as limits on international collaboration may lead to stifling of innovation. Participants voiced concerns related to the potential erosion of trust between institutions and their (multinational community of) researchers.

5. Participants highlighted the difficulties associated with due diligence re the recruitment of research colleagues, and highlighted concerns about the treatment and wellbeing of colleagues and collaborators whose nationality or heritage has been labelled as being from a ‘country of concern’ and the danger of a climate of suspicion developing around valued colleagues.
How can guidance and advice to researchers be improved?

1. **Active participation by UKRI**: Participants said it would be helpful if UKRI provided guidance/training on Trusted Research aspects of grant applications.
2. **Improve accessibility and understanding** of Trusted Research issues, which are currently difficult to understand and access.
3. Creation of a **centralised system and set of resources**: A ‘one stop shop’ with centralised set of good practice guidelines and resources would bring uniformity to the approaches that UK institutions can take.
4. **Funding provision and resources**: Participants noted considerable costs of developing and implementing Trusted Research policies; government grants might facilitate the creation, accreditation and ongoing review of Trusted Research capacity within universities.

What could institutions do to manage risks and help individual researchers?

1. Participants noted the **need for culture change** when it comes to issues of Trusted Research, as many researchers are not aware of the implications for their work. Suggestions included tailored guidance for different communities.
2. Participants suggested that institutions should introduce **mandatory, contextual training** for all staff along with accessible resources which include details of specific points of contact and timelines.
3. Create a **Trusted Research community**: Community-level action and a collective approach would serve as a powerful mechanism to establish shared values and actions.
4. Create **institutional registers**: Several suggested the creation of institutional registers to cover topics such as risks and trusted collaborators, though others noted potential risks (e.g., the implied ‘trustworthiness’ of individuals based on their collaborators/connections).
5. Institutions should communicate the **value of research support functions** to the research community and invest in appropriate resource and training to these colleagues to enable them to better advise academics as part of their usual research support activities.

Concluding remarks

Despite the limitations of the format, we were able to gather a range of ideas and impressions, in a short space of time, from a diverse pool of academic researchers, including some constructive suggestions for next steps.

Our experiences in organising the workshop also raise a couple of flags: it was **hard to recruit participants for this workshop** even via security-relevant UK academic networks. If even those researchers with a self-identified interest in security matters will not commit to a half-day workshop it will be difficult to gain the attention of those who may not see themselves as doing security-relevant research. We also noted that among those who do recognise the importance of the issues, there may be some **over-confidence about their understanding**. That is, they may be familiar with some elements of Trusted Research but have only partial or no awareness of other aspects of what is considered within the scope of Trusted Research. Unconscious lack of awareness may be another barrier to achieving wide-spread understanding and adoption of new policies and procedures.
How do researchers understand “Trusted Research”? Workshop
Findings

Introduction: The Trusted Research Context

The aim of this workshop was to identify ways to improve researcher awareness of issues related to
“Trusted Research”, an umbrella term that includes issues related to:

- Regulatory compliance (e.g., Export Controls, the Academic TA Scheme, GDPR, partner-
country regulations)
- Protecting IP (including cyber security and data protection issues)
- Conflicts of interest with other research partners
- Risk of foreign interference in research/teaching and academic freedom
- Protecting staff and students overseas
- Reputational risk and ethical issues (including potential misuse/abuse/dual use of
research knowledge)

Although anxieties about risks to research integrity and foreign interference are not new, in recent
years such concerns have become increasingly prominent, particularly in the context of international
academic collaborations.

The issues touch multiple stakeholders, with multiple interests, some of which are in tension. In
central government, Trusted Research issues raise policy concerns for defence and national security
(the UK Intelligence Community, particularly the Centre for Protection of National Infrastructure –
CPNI1, the National Cyber Security Centre - NCSC2, Home Office, Ministry of Defence), industrial
strategy and trade (Department for Business, Energy & Industrial Strategy - BEIS3), foreign policy
(Foreign Commonwealth and Development Office) and education (Department for Education). Within
the academic community, UK Research and Innovation - UKRI, Universities UK4 and the Russell Group
are all involved in Trusted Research policy work. In addition, research groups such as the Academic
Freedom and Internationalisation Working Group5 and the Policy Institute at Kings College London6
have made useful contributions to understanding specific issues within the Trusted Research ambit.

Concerns about threats to research have become increasingly prominent in Parliament, think tanks,
and in press coverage that has highlighted potential espionage threats to Covid-19 vaccine research,
concern over legal risks for individual academics, and worries about threats to academic freedom7.

---

1 https://www.cpni.gov.uk/trusted-research-guidance-academia
2 https://www.ncsc.gov.uk/blog-post/trusted-research
3 https://questions-statements.parliament.uk/written-statements/detail/2021-05-25/blls52
4 https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/managing-risks-in-internationalisation.aspx
5 https://hrc.sas.ac.uk/networks/academic-freedom-and-internationalisation-working-group
6 https://www.kcl.ac.uk/policy-institute/research-analysis/the-china-question, https://www.research-
s/catalogue-of-case-studies-on-intangible-technology-transfers-from-universities-and-research-institutes
At the same time, post-Brexit Britain is seeking to maintain and enhance its position on the world stage, with the strong message that Britain is “open for business”⁸. International collaboration is at the heart of ambitious government strategies for industry, science and technology, and education. In education, the government seeks to increase UK education exports and attract increasing numbers of international HE students into the UK². The huge benefits that colleagues from around the world bring to academic research and innovation are widely recognised. Not collaborating with international partners is not an option.

The university sector needs to maintain and develop international collaboration while also protecting research integrity. This tension between being “outward looking” and being “on guard” raises significant challenges for the sector, including:

- Understanding partnerships and what is meant by ‘due diligence’ in a changing world
- Protecting intellectual property
- Protecting reputation and autonomy
- Protecting staff and students
- Protecting benefits of international collaborations including innovation and research excellence
- Protecting income from research collaborations and international students
- Coping with increasing bureaucracy and control

There is a fear that if the sector cannot demonstrate it is managing risks to the satisfaction of government, then more regulation is coming. We have already seen the expansion of Academic Technology Approval Scheme (ATAS)¹⁰ to include researchers as well as students from 2021, and in the May 2021 Queen’s Speech, the government announced a consultation on proposals to introduce a UK Foreign Influence Registration Scheme¹¹. Similar provisions introduced by the Australian government in the Foreign Relations Bill 2020 have reportedly caused difficulties for universities, with concerns about compliance bureaucracy, constraints on institutional autonomy and threats to current and future international collaboration¹².

Much has been done already to support the work needed to address the many practical and policy concerns for universities raised under the Trusted Research umbrella. At a strategic level, CPNI/NCSC and Universities UK have issued guidance aimed at senior leaders¹³. A UUK Conference in November 2020 facilitated the discussion and sharing of good practice as well as the identification of strategic challenges¹⁴. Many UK universities are actively working on adapting and rolling out the guidance while others are considering the implications for their processes.

Although robust policies and procedures will be at the heart of implementing Trusted Research measures (broadly defined), ensuring that those policies and procedures are followed will depend largely on the behaviour of individual researchers. CPNI/NCSC has issued guidance for Principal

---

¹⁰ https://www.gov.uk/guidance/academic-technology-approval-scheme
¹⁴ https://www.universitiesuk.ac.uk/events/Pages/Safety-and-risk-management-in-higher-education.aspx
Investigators (PIs) and research teams, but awareness and uptake of this guidance is patchy. Amid all this welcome activity around Trusted Research in the last couple of years, relatively little attention has been paid to seeking the views of individual researchers.

The workshop

The SPRITE+ Trusted Research workshop in March 2021 explored the implications of current guidance for ‘front line’ PIs and their teams, examining the barriers to awareness and implementation, and suggesting ways to improve the situation.

The workshop was advertised to members of SPRITE+ and to members of other security-relevant academic networks, hubs, and institutions. 37 individuals from 21 institutions volunteered to join the workshop. They came from a range of career stages and research disciplines. Although several participants had extensive experience of security-relevant research, many others had little experience or awareness of Trusted Research issues.

The workshop featured context-setting short talks from Professor Sir Peter Gregson (VC of Cranfield University and Universities UK lead for Trusted Research), Professor Emma Barrett (Director SPRITE+), and Professor Anthony Finkelstein (Chief Scientific Advisor for National Security), but most of the workshop time was spent in breakout group discussions.

Summary of breakout discussions

Two rounds of breakout discussions focused on the following topics, which were identified in advance by the SPRITE+ team through discussion with relevant stakeholders, and an analysis of reports and articles discussing Trusted Research issues:

- Protecting reputation and values
- Well-being, safety and security of people and partners
- Cyber security
- Protecting research integrity
- Regulatory compliance

Participants focused on identifying relevant issues, concerns, and good practice. Regardless of their current role, participants were asked to consider the issues from the perspective of an academic researcher, with a focus on activities related to potential and actual external research collaborations, including joining funded projects as a collaborator, leading a collaborative project, recruiting PhD students, and engaging with other researchers outside the University.

Participants made shared notes of their discussions during their breakout sessions. After the workshop, the SPRITE+ team grouped the notes into themes across participants and identified the following themes. Note: See Appendix 1 for a transcript.

Key areas of risk and concern

1. **Lack of awareness of guidance/support available**

Participants reported little awareness of the guidance available to help researchers protect their work. This extended to concerns over the roles of individual researchers and their institutions in ensuring appropriate due diligence. Participants noted issues related to reputation and values,
recruitment, and capacity and capability of hostile actors as areas of particular concern where further guidance is required.

2. Inconsistencies in approaches

Participants did not believe that there is a consistent approach to dealing with Trusted Research issues across different universities, and between universities, government, and industry. Differences in approach for different disciplines were reported: many universities appear to be focused primarily on risks in STEM disciplines, which may lead to neglect of risks associated with social science and humanities disciplines (often perceived as less ‘risky’ in the context of Trusted Research). As interdisciplinary research grows, the scope of what needs to be protected is also potentially growing.

3. Impact on funding opportunities and grant management

Participants reported increasing pressure to engage in international collaborations and some reported a perception that researchers may feel they have no choice but to collaborate. Participants were unaware of any UKRI guidance on TR issues and did not believe that UKRI currently require TR due diligence in the bid application process. Typically, due diligence processes such as the implementation of research contracts and NDAs begins after a grant has been won. Where these are necessary, participants reported they can be problematic for researchers as they can: (1) slow the pace of research, which can lead to the loss of valuable collaborators and reputational risk; and (2) be so administratively burdensome that they outweigh the value of the research award.

4. Limitations on academic freedom

Participants raised concerns about potential limitations on academic freedom and the ability of researchers to explore and innovate. These were framed in terms of how limits on international collaboration may lead to stifling of innovation. Participants voiced concerns related to the potential erosion of trust been institutions and their (multinational community of) researchers if guidelines and regulations become too stringent.

5. Employment and treatment of individuals and prospective partners

Participants highlighted the difficulties associated with the recruitment of research colleagues, with the burden to ensure appropriate due diligence resting with academics who feel they are inadequately supported. Participants also highlighted concerns about the treatment and wellbeing of colleagues and collaborators whose nationality or heritage has been labelled as being from a 'country of concern' and the danger of a climate of suspicion developing around valued colleagues. There is an important distinction between the beliefs, intentions, and behaviours of individuals versus those of a state.

How can guidance and advice to researchers be improved?

Several consistent themes emerged as participants discussed how guidance and practice could be improved:

1. Active participation by UKRI as a major UK research funder

Participants suggested that, as a major funder and a trusted, semi-independent body, it would be helpful if UKRI provided guidance/training on Trusted Research aspects of grant applications. It was suggested that a Trusted Research checklist could be embedded within the grant application process to ensure that due diligence procedures are completed early on in the development of research.
projects. This checklist could be affiliated with existing UKRI compliance procedures and aspects of the Research Integrity Concordat.

2. **Improve accessibility and understanding of Trusted Research issues**

Some participants were aware of the Trusted Research resources currently available, but many reported that understanding and accessibility of the issues presented is limited. Participants suggested that resources could be better tailored to individuals depending on their role e.g., students, research staff, professional services staff. Some groups suggested that the use of case studies and scenario-based training could help to contextualise issues for researchers and a traffic light system could highlight key risks. One suggestion was a decision tool, where researchers would answer questions about their research and be directed to the most appropriate resource depending on their answers. Some institutions already have such a tool to help researchers judge the right level of ethical approval for research; this could be adapted to include questions about TR risks.

3. **Creation of a centralised system and set of resources**

The current mix of organisations who are connected to or have a stake in Trusted Research policies can be confusing. A ‘one stop shop’ could simplify matters. The creation of a centralised set of good practice guidelines and resources would bring uniformity to the approaches that UK institutions can take. This in turn, could lead to better collaboration between researchers working across different disciplines, organisations and sectors. Participants also suggested that a centralised register may be useful for the sector to demonstrate compliance, and the creation of a national forum could serve as a vehicle to surface and discuss issues.

4. **Funding provision and resources**

Participants noted that the creation and implementation of Trusted Research policies within institutions is not a trivial exercise and requires time, resource, and money. The cost of setting up secure facilities is not inconsiderable and there is currently no additional funding available to support these activities. It was suggested that government grants might facilitate the creation, accreditation and ongoing review of Trusted Research capacity within universities.

What could institutions do to manage risks and help individual researchers?

1. **Facilitate culture change**

Participants noted the need for culture change when it comes to issues of Trusted Research, as many researchers are not aware of the implications for their work. Institutions should communicate new policies and guidance so that it resonates with the research community e.g., by providing answers to questions such as “what are the risks?”, “what are the threats?”, “how will this policy help me?” and so on. A ‘stepped’ model should be considered, with step one being basic knowledge that everyone needs, followed by higher steps for intermediate and advanced aspects for specialists.

2. **Provide accessible resources**

Participants suggested that institutions should introduce mandatory, contextual training for all staff along with accessible resources which include details of specific points of contact and timelines. Some participants noted that it is often difficult to know who to seek guidance from on a particular issue.

---

16 Since the workshop, the government has announced the establishment of a Research Collaboration Advice Team, a “new unit to deal with risk of foreign espionage and theft of IP from universities”, see https://sciencebusiness.net/news/uk-announces-new-unit-deal-risk-foreign-espionage-and-theft-ip-universities
Institutions should take ownership of their training materials and ensure that they are continually updated.

3. **Create a Trusted Research community**

Participants noted the need to think broadly and to go beyond individual researchers, disciplines, and institutions. Community-level action and a collective approach would serve as a powerful mechanism to establish shared values and actions.

4. **Create institutional registers**

Several of the groups suggested that the creation of institutional registers to cover topics such as risks and trusted collaborators. However, participants did recognise the potential issues that might come with such registers e.g., the implied ‘trustworthiness’ of individuals based on their collaborators/connections.

5. **Increase the capacity of research support functions**

Participants noted that institutional support functions enable the delivery of high quality research but are often limited in capacity and knowledge. Institutions should communicate the value of these functions to the research community and invest in appropriate resource and training to these colleagues to enable them to better advise academics as part of their usual research support activities.

**Concluding remarks**

A few observations to conclude. First, we acknowledge that there are, of course, limitations to our workshop findings. Although our participant group was reasonably diverse, it cannot be considered a random or unbiased sample. As such, our findings should be treated as exploratory rather than definitive. Further research with the research community (e.g., surveys, interviews, focus groups), would develop our understanding.

Nevertheless, we were able to gather a range of ideas and impressions, in a short space of time, from a diverse pool of academic researchers, including some constructive suggestions for next steps. We are aware from stakeholder discussions that many of the comments from participants (for instance, confusion and lack of awareness about existing guidance; anxieties about academic freedom; concern about bureaucracy), will not be a surprise to those involved in setting Trusted Research policy. However, the issue of the wellbeing of researchers whose heritage is from a ‘country of concern’ is not one that has been mentioned previously in stakeholder discussions. Anecdotally, we have heard of colleagues of Chinese, Iranian and Russian heritage feeling uncomfortable about or even humiliated by the tone of some conversations and media stories about the involvement of ‘hostile states’ in UK academia. Systematic research may be necessary to understand how widespread these experienced are, but the well-being of international colleagues is clearly an important consideration in developing and implementing Trusted Research guidance going forward, both as a matter of principle and to ensure buy-in from researchers.

Our experiences in organising the workshop also raise a couple of flags. Recruiting participants for this workshop proved to be more difficult than anticipated, despite extensive advertising around all the most significant security-relevant UK academic networks (Academic RISC, CREST, Petras, the NCSC-funded Research Institutes etc). This highlights the challenges the sector may face going forward: if even those researchers with a self-identified interest in security matters will not commit to a half-day
workshop it will be difficult to gain the attention of those who may not see themselves as doing security-relevant research.

Finally, among those who do recognise the importance of the issues, there may be some over-confidence about their understanding. Before the workshop, we polled participants for their level of confidence in understanding Trusted Research and its relevance to their work. Of those who responded, a little over half said they were confident or strongly confident. While this is an informal poll and the numbers are small, we noted from the discussions that some of these participants may have been over-confident about their understanding. That is, they may be familiar with some elements of Trusted Research but have only partial or no awareness of other aspects of what is considered within the scope of Trusted Research. Unconscious ignorance and over-confidence may be another barrier to achieving wide-spread understanding and adoption of new policies and procedures.
Appendix 1: Detailed feedback from breakout discussions

Participants in breakout rooms were encouraged to discuss relevant issues and make notes on virtual ‘sticky notes’ in two rounds of discussions. The contents of the notes have been transcribed below. They have been lightly edited to remove identifying particulars and for clarity. Some notes captured an emerging group view and others reflected the views of a single participant. Where they discuss risks and concerns, the notes reflect participants’ *perceptions* of risks/concerns, and may not be an accurate reflection of actual risks/concerns.

Protecting reputation and values

The following issues were considered under this theme:

- Due diligence that includes reputational, ethical and security risks.
- Ongoing monitoring and review
- A culture that enables staff to raise concerns about potential or current partnerships
- Ensuring partnerships do not compromise core values such as academic freedom and freedom of speech, resisting attempts at interference and influence

**Key risks/issues**

- Potential to limit academic freedom and the ability of researchers to innovate.
- Potential loss of research income if barriers to collaboration are created.
- CPNI Trusted Research guidance on non-academic partner due diligence directs readers to the US export entity control list. There should be a UK list made available for UK universities to refer to.
- Potential to erode trust between individual researchers and institutions.
- There is little awareness of and focus on issues beyond on cybersecurity, meaning that other areas become more vulnerable to attack.
- Limited guidance available relating to reputation and values. Lack of understanding as to where the responsibility falls to manage the reputational impact when mistakes are made.

**Suggestions for how guidance and advice to researchers could be improved**

- Timeliness and clarity of responses needs to be prompt/improved, particularly when particular/specific issues arise.
- The use of a traffic light system on potential risks could improve understanding and accessibility.

**Suggested actions that institutions could take to manage risks and help individual researchers**

- Develop their own codified values and ethics statements, which are transparent and publicly available. Note the need to be careful, however, that policies don’t get in the way of academic engagement with narratives related to changing society for the better.
- Institutional risk registers to enable academics to understand the liabilities within the research domain.
- An institutional register of collaborations. However, this comes with other issues, for example, the implied trustworthiness of a given researcher given their collaborators/connections.
Well-being, safety and security of people and partners

The following issues were considered under this theme:

- Researchers working in sensitive areas whose research may be the subject of attempted theft or compromise.
- Researchers working on potentially sensitive collaborations and/or on multiple collaborations where different partners may be competitors.
- Researchers traveling overseas to visit collaborators / potential partners
- Researchers (and other staff) working in the UK whose nationality or heritage is from a country deemed by the UK state to be a country of concern
- A culture that enables staff to raise concerns about potential or current partnerships

Key risks/issues

- Lack of awareness of and training/policies on risks and threats within universities. Lack of understanding as to what constitutes sensitive research.
- Personal risks, particularly concerns around the negative impacts from errors despite institutional training around export controls.
- There is no UKRI position on these issues and they do not provide guidance and/or training.
- Lack of understanding about who can give specific advice and concerns of who researchers should and shouldn’t be speaking to.
- Limited research funding from UK Government, meaning that funding may be only available from foreign governments and there is no other choice but to collaborate.
- There is a struggle to generate interest for some postgraduate courses from within the UK. There is much more interest from foreign students.
- Individual PIs are responsible for making decisions on who to collaborate with, which PhD students take on.
- There is a disconnect between national security interests and University / research funding imperatives.
- There is no systematic approach to identifying who is 'safe' to hire. The reliance on academics to identify 'suitable' candidates is flawed as approaches will differ, level of checks and motivations will vary. The worst case scenario is to have a whole UKRI project populated by 'adversaries', from PI down, with UKRI funding lending credibility.
- There is nothing in the guidance that takes account of how people whose nationality or heritage is from a 'country of concern' feel (and are treated) by colleagues. Assumptions are made about individuals but they may have very different beliefs and values from their government. It can be hurtful to be labelled (or feel you've been labelled) as 'suspicious' or a potential threat.
- Risks to the personal safety of staff and participants. Safeguarding and prevention of threat to researchers abroad is crucial.
- Even within UK, poor judgement on publicising research being undertaken can lead to unwelcome attention by actors with criminal intent e.g. human traffickers, cyberattackers.

Suggestions for how guidance and advice to researchers could be improved

- Creation of a ‘one-stop shop’ rather than a mix of organisations (e.g. CPNI, NCSC, BEIS), which can be confusing.
• Replication of the NCSC ‘0800’ info line across other disciplines.
• Embed Trusted Research check in grant application process at UKRI.
• Create a systematic approach that brings uniformity to the approaches that UK institutions can take, e.g. across the Russell Group and other institutions.
• Ensure timely advice and guidance, and transparent processes to enable due diligence checks to be performed early.
• Provide both strategic and tactical guidance (i.e. what to do and not (Strategic), and also how to (Tactical)).
• Universities provide advice on handling the press. They should be under a similar obligation to give advice on Trusted Research.
• When recruiting new staff, the availability of a centralised system to ensure security clearance without academics having to do all the background detective work would be useful.

**Suggested actions that institutions could take to manage risks and help individual researchers**

• Sensitisation to ‘dual use’ problem, and ability to weigh up options, e.g. will this research serve a purpose where the positives of intended use outweigh the risks of a secondary (negative) use.

• Personal safety risks varies by country. Availability of ‘academic tradecraft’ training would be useful to enable staff to spot insider threats, safety risks, travelling overseas, etc. This training is currently delivered by Cranfield to ‘MOD’ academics, but would be valuable for UK institutions to raise awareness and skill as default training for research personnel. Using real-life case studies would inject interest and ‘make it real’.

**Cyber security**

The following issues were considered under this theme:

• On and off campus, in the UK and overseas
• Preventing unauthorised access, disclosure, destruction, or alteration of data including Intellectual property, commercially sensitive information, personal identifiable data, financial data

**Key risks/issues**

• Inconsistencies in approach across different universities e.g. some universities have tight centrally-controlled IT policies e.g. on password changing and software installation, whereas other universities have less central control.

• Whilst universities seem to be taking cybersecurity seriously, a balance is required to allow researchers to access software/data. Over management of IT resources can lead to employee / researcher resistance.

• Cybersecurity practices only cover the ‘admin’ or ‘teaching’ tech within universities and doesn't cover the research kit which academics maybe building.

• Researchers are not always aware of the resources available and may not understand that their research requires protection. Researchers are not aware of the capacity and capabilities of hostile actors, which can be extremely sophisticated.
The scope of what needs to be protected has grown e.g. in the past, researchers working on biological agents knew (generally) that they needed to be careful but what about topics such as facial recognition where there is dual use and unethical applications?

Researchers may not understand the value of the IP they are generating – publication of open source code/tech design confuses the issue.

Further confusion when collaborating as a Co-I with international partners due to differing standards, controls and tolerance for flexibility/risk. There is a need to identify solutions that allow for secure collaboration. People 'work around' and work insecurely because there is no apparent alternative or 'how to' guide on best practice.

There are issues for researchers travelling overseas. There is little appreciation of the risks e.g. not just 'obvious' countries like Iran or China, but also US government powers are of concern. Laws in other counties enable states to compel visitors to unlock laptops etc.

Lack of understanding about the role of managers/mentors to reinforce messages and good practice.

Suggestions for how guidance and advice to researchers could be improved

- Research projects should be required to obtain cybersecurity approval as well as ethics, data protection etc.
- Tailored guidance like the FCO country guidance for example.
- Create a national forum as a vehicle to surface and discuss issues.
- Provide a series of case studies to describe what can go wrong to help motivate researchers to take notice.

Suggested actions that institutions could take to manage risks and help individual researchers

- Increase the capacity of university research support functions and emphasise their value to researchers as opposed to “a necessary evil”. Improve training for professional staff to enable them to better advise researchers working in this area.
- Identify a way to explain the basis of new security guidance so that it resonates with researchers e.g. what is the risk, what are the threats, how will the change help me.
- Review policies on visitors and ensure guidelines are clear about individual responsibilities.
- Cyber physical convergence - IT security and physical security (and maybe personnel security) should not be treated separately.
- The cost of setting up secure facilities is not inconsiderable - can government give grants to universities to set them up, and help with accreditation and ongoing review?
- Look to other sectors where security/safety is a core concern and how they ensure the right culture and practice.
- Need to build on existing process and integrate where possible rather than invent new ones. Ethics process is well established and understood, so this could be a good place to build from. There is a need to think about disciplines/areas where ethics is not a routine consideration. Also, there is often no routine audit or penalties for non-compliance.
- Create an ‘amnesty’ for researchers to surface workarounds/concerns/bad practice, and a (a) no-blame approach and, (b) consider how to deal with academics who won’t want to report a mistake because they don’t want to be stopped.
- Consider a ‘stepped’ model - basic knowledge that everyone needs, intermediate and then advanced (for specialists in this area who then help those at basic/intermediate).
- Encourage / facilitate networking across and between universities to share experiences, good practice, ideas etc. so we don’t reinvent wheels

Research integrity

The following issues were considered under this theme:

- Due diligence that includes reputational, ethical and security risks
- Preventing theft of intellectual property
- Maintaining research integrity (quality, independence etc.)
- Maintaining confidence of partners when working on multiple collaborations where different partners may be competitors.
- Protecting robust collaborations and clear exit strategies
- Ongoing monitoring and review

Key risks/issues

- Differing standards for what constitutes a 'trusted researcher' within the government, industry, and academia.
- Lack of understanding of the risks associated with some humanities disciplines, which are often perceived as less risky. However, students/researchers are not constrained by disciplinary boundaries.
- Uncertainty as to whether or not all universities sign up to trusted research practices - voluntary or mandatory and the consequence of this to distribution of research.
- The research ethics processes can be both helpful (in identifying good practice) but also constraining as it can be too one-size-fits all and risk averse, and not able to deal with nuances of a particular research context.
- NDAs, research contracts etc. slow the pace of research.
- Risk that risk-adverse administration could disproportionately reduce research outcomes/activity/income. Often 1-to-1 researcher trust relationships that cannot be verified by the Institute may become issues e.g. a researcher lost a once in a lifetime opportunity and the trust of an international partner who was 'offended' at the assessment of their integrity.
- Lack of understanding as to whether research students are vetted, how the process works and if it’s fair.
- There is a risk that clamping down to reduce risk in some areas will lead to increased activity in others.
- The community of PIs in an institution probably lack awareness and may resist anything that limits freedom and flexibility in their research. There is a need to understand how to introduce culture change.
- The risk is probabilistic rather than just trusted/untrusted. We’re typically very bad at estimating risk. For the higher-grade threats, the level and nature of the threats is only available to the Intelligence community.
- Concerns about how the costs of implementing trusted research practices are to be met e.g. a block grant from funders?

Suggestions for how guidance and advice to researchers could be improved

- Recognise that this is not a binary issue. There is a need to apply a 'grey-scale' of risks and mitigations.
• Provide case studies and scenario based training.
• Draw lessons from any other interventions or processes already in place e.g. information security, UKRI compliance, and aspects of the Research Integrity Concordat.
• Create a strategy for collaborating with international (and multi-national) industrial partners.

Suggested actions that institutions could take to manage risks and help individual researchers

• Auditable frameworks for risk evaluation with categorisation of potential ‘mal-intervention’.
• There is a need for community level action - a collective approach to establish shared values and steps for action.
• There is a need to think broadly and go beyond individual researchers and institutions, but, recognise that some in the community may already be compromised and/or also reluctant to lose current funding.
• Actions/frameworks can’t be implemented top down and can’t be bottom up either; they need to be implemented on multiple levels at the same time. A graded approach could be manageable, based on level of risk.

Regulatory compliance

The following issues were considered under this theme:

• Legislation and regulations, contractual arrangements etc.
• Export controls, Academic Technology Approval Scheme etc.
• Legislation/regulation in countries where collaboration partners are based (extraterritorial jurisdiction).
• Due diligence to ensure partners are who they say they are, root out bad faith actors.
• Ongoing monitoring and review.

Key risks/issues

• Consideration of time limits - it takes months to engage with partners and arrange contracts, which can limit opportunities to apply for funding due to tight deadlines. Concerns that the burden of the administrative process will outweigh the value of a contract. Potential to affect reputation.
• Difficulties in implementation of a standard process across disciplines, which may impact flexibility.
• There is a need to communicate across nationalities without appearing hostile.
• Research data management requirements differ across funders.
• Some legislation implemented can impact on areas where it shouldn't be relevant e.g., recruiting PhD students in areas where there aren’t reported security risks. This can cause significant delays, leading students to withdraw their applications or find alternative positions.
• Sometimes risk only becomes apparent part-way through project.
• Regional boundaries and the movement of data out of region. Concerns about how to access data and ownership, particularly when it is stored in another country.
• There is no central register of compliant or trusted individuals/partners. If such a register existed, that are issues concerning ownership, should it be a consortium of universities or a governance body?
Suggestions for how guidance and advice to researchers could be improved

- A central body should capture the pillars of Trusted Research.
- Learnings could be taken from the Data Security Protection Tool kit framework (health research).
- Creation of a central register that agencies could sign up to and demonstrate compliance.
- Provide contextually appropriate/directed advice, including detail of the intended learning outcomes. The guidance should be tailored for students/staff compared to senior management.

Suggested actions that institutions could take to manage risks and help individual researchers

- Mandatory, context-appropriate training.
- Provide case studies to describe what researchers can and can’t do.
- Provide accessible resources, including details of who to contact, time implications, etc., which is continually updated/maintained. Institutional ownership.
Appendix 2: SPRiTE+, the UK Security, Privacy, Identity, and Trust Engagement NetworkPlus

SPRiTE+ brings together people involved in research, practice, and policy with a focus on digital contexts. We are a ‘one stop shop’ for engagement between academic and non-academic communities, and a platform for building collaborations across the spectrum of issues relating to the future of digital trust, identity, privacy and security.

Membership of SPRiTE+ is free, and open to anyone involved in exploring the future of TIPS, including academic researchers, industry, government, law enforcement and civil society organisations. Academic researchers make up 75% of our total membership (600+ and growing) with >90 higher education institutions represented and a broad mix of research expertise including technical, scientific, and social science disciplines.

SPRiTE+ is primarily a vehicle for collaboration – a way for academic and non-academic communities to connect and communicate. We facilitate engagement around any topic that is related to digital security, privacy, identity, and/or trust. This might be to gain expert advice, to find partners for specific projects, or to share expertise with others.

Activities

We facilitate connections and knowledge sharing through:

- Reaching out to our SPRiTE+ Members and Expert Fellows to request input/resources/expertise, via our newsletter and mailing list, or more targeted communications
- Hosting online workshops, town halls, sandpits, and focus groups via an open or targeted invite to the SPRiTE+ Membership and Expert Fellows community. We make use of breakout rooms for discussion and capture the outputs in real time. (When Covid restrictions allow, we will also co-host in-person events or activities.)
- Co-organising hackathons, sprints, and similar challenge events
- Co-organising public engagement activity, such as exhibitions, talks, festivals, competitions, events for schools or workplaces
- Sharing and championing the activities of members, including via social media
- Supporting internships and attachments, for instance allowing SPRiTE+ Members to work with non-academic organisations to explore a specific issue relevant to SPRiTE+ (e.g., a short research assignment or knowledge transfer activity).

Research: We use the SPRiTE+ Research Fund to support working groups, feasibility studies and short projects, which are co-created with end-users. We have an annual funding call for new projects.

Events: We also organise one-off events, often in partnership with related organisations, for example:

- Marginalised communities’ experiences of digital technologies
- Exploring ‘Digital Responsibility’ in cyber security (with RISCS)
- Raising awareness of Trusted Research guidance (with CPNI)

Resources: We have curated online education and awareness resources which can be accessed via our website. Some of these materials are targeted at ‘first timers’ and offer a general introduction to relevant areas, and others provide a deep dive into more advanced topics for established stakeholders.

https://spritehub.org/ admin@spritehub.org Twitter @SpritePlus
Guidance and support: We offer information and guidance to Members applying for grants and have a programme to support early career researchers.

Leadership and funding

SPRITE+ is led by a consortium of five universities: University of Manchester (lead institution), Imperial College London, Lancaster University, Queen’s University Belfast, and University of Southampton. We are supported by 15 non-academic Project Partners from different sectors, including industry, government, law enforcement, and civil society.

We are funded until 31 August 2023 by the Engineering and Physical Science Research Council as part of its Digital Economy programme (grant reference EP/S035869/1).

More details:

- Website: [https://spritehub.org/](https://spritehub.org/)
- Twitter: [https://twitter.com/spriteplus](https://twitter.com/spriteplus)
- LinkedIn: [https://www.linkedin.com/company/spriteplus](https://www.linkedin.com/company/spriteplus)
- Email:
  - General enquiries: admin@spritehub.org
  - Director: Professor Emma Barrett emma.barrett@manchester.ac.uk
  - Network Manager: Dr Natalie Theodoulou natalie.theodoulou@manchester.ac.uk