TRUSTED RESEARCH

Evaluation Framework

National Protective Security Authority

National Cyber Security Centre

Contents

Introduction

NPSA and NCSC developed the **Trusted Research Evaluation Framework** in consultation with experts across the academic sector and within relevant parts of government. The Trusted Research Evaluation Framework helps academic institutions at various stages of their journey to reach a mature approach to research security.

This document serves as a tool for maturity self-assessment, and is designed to complement existing Trusted Research guidance available from the NPSA website.

Before using the Trusted Research Evaluation Framework, you should first read the accompanying **Trusted Research Evaluation Framework – user guide**.

Endorse: senior endorsement and governance

Endorse: senior endorsement and governance

Senior sponsor: Trusted Research

Foundation ○

You have a named executive/board-level owner who is responsible for the risks associated with Trusted Research (research security risk) as well as an academic lead for Trusted Research.

Intermediate ○ ○

The executive/board have discussed the risk associated with Trusted Research and it forms a regular item on the board agenda.

Developed ○ ○ ○

You have a policy and process to define your institutional risk appetite for international collaborations, which will feed into risk register decisions. Board governance and risks documentation sets out the institution's risk appetite and policy in relation to Trusted Research. These are reviewed on an annual basis.

Senior sponsor: Network

Foundation ○

A named executive/board-level sponsor and academic lead are responsible and accountable for the security of network and information systems, regularly reporting to the board, council, court or equivalent governing body.

Intermediate ○ ○

You have an identified technical lead reporting to a member of the board and can evidence that they take technical advice from them.

Endorse: senior endorsement and governance

Leadership culture

Foundation ○

Your institution's Trusted Research senior owner sets the tone and culture for an institution-wide approach to research security, acting as a champion for good practice. This may include senior comms, e.g. online newsletters/ departmental bulletins, blogs or opinion pieces on your intranet site etc.

○

Intermediate ○ ○

Your institution's senior leadership team sets the tone and culture for an institution-wide approach to research security, acting as a champion for good practice. This may include senior comms, e.g. online newsletters/departmental bulletins, blogs or opinion pieces on your intranet site etc.

○

Developed ○ ○ ○

Leaders within the institution, from the top down to department heads and senior researchers, set the tone and culture for an institution-wide approach to research security, acting as champions for good practice.

○

Institutional risk appetite

Foundation ○

You have a governance or decision-making group or groups which review high-risk research, innovation, and collaboration.

○

Intermediate ○ ○

You have a governance or decision-making group or groups which review high-risk research, innovation, and collaboration, as well as funding and philanthropy, and make decisions on those risks or the suitability of mitigations.

○

Developed ○ ○ ○

Your annual report on institutional risk appetite includes Trusted Research considerations.

○

Endorse: senior endorsement and governance

Compliance

Foundation ○

You have specific members of staff and senior sponsors responsible for areas touching on Trusted Research concerns, including ATAS/visas, IP protection strategy, NS&I notifications, export control, the National Security Act and overall research risk.

Intermediate ○ ○

Your institution regularly engages with the legislation and policies relevant to Trusted Research issues: ATAS/visas, copyrighting and patenting, NS&I notification, export license, the National Security Act and end user applications.

Developed ○ ○ ○

Your institution maintains a central record to ensure institutional-level understanding of engagement with the aforementioned legislation and policies.

Encourage: communications

Encourage: communications

Internal comms strategy

Foundation ○

You have an accessible internal communications strategy for safe, secure and responsible research and innovation.

○

Intermediate ○ ○

You have an internal communications programme which promotes awareness of the Trusted Research campaign and your institutions' policies in relation to managing research security risks.

○

Developed ○ ○ ○

Research security culture is actively and positively a part of research at your institution, with senior role modelling and visible active compliance, for example staff survey results and regular reviews in research.

○

Wider Trusted Research links

Foundation ○

You encourage access to the Trusted Research campaign materials and social media assets.

○

Intermediate ○ ○

Your institution's external website and/or internal intranet promotes the full range of Trusted Research assets.

○

Developed ○ ○ ○

Your institution can demonstrate active engagement in sector-wide workshops on sharing Trusted Research practice for example the Trusted Research STEM Forum, professional body events, and hosting their own events.

○

Encourage: communications

Institutional role modelling

Foundation ⊙

You have an external webpage and internal intranet site that provide information to visitors and guidance to staff on the institution's commitment and implementation of trusted research principles.

○

Intermediate ⊙ ⊙

Your external website promotes Trusted Research as a valued, positive element of research at the university.

○

Developed ⊙ ⊙ ⊙

Your external website promotes Trusted Research as a valued, positive element of research at the University, advertising examples of good practice, managed risks, and lessons learned from within your institution, but not to the detriment of information protection where relevant.

○

Educate: training

Educate: training

Training provision

Foundation ⊙

You run training on Trusted Research principles incorporating collaborations, due diligence, dual use technology and IT security alongside legal obligations under export control, knowledge assets, GDPR, NS&I, the National Security Act and other relevant legislation for all academic staff.

Intermediate ⊙ ⊙

You run induction and regular refresher training on Trusted Research for academic staff including visiting academics which they are required to attend.

Developed ⊙ ⊙ ⊙

You have a range of education and awareness activities (such as workshops, presentations, talks, roundtable exercises) to promote awareness of Trusted Research and the university's own policies and process on research risk, legal obligations, travel and IT security, and can evidence that all researchers engage with the guidance and understand their responsibilities.

Your research office or Technology Transfer Office, alongside the senior risk owner, work to promote awareness of Trusted Research throughout the institution.

You have an internal team or identified roles who are focused on Trusted Research and work in support of a senior owner to co-ordinate a behavioural change programme, deliver training, promote raising awareness, maintain risk logs and develop and update relevant policies.

Those responsible for Trusted Research compile quarterly updates for the senior risk owner on research security risk and provide regular updates on risk levels to the board. Research security is promoted as a positive and important career path and enabler within the university's wider research office support function.

Educate: training

Personnel security training
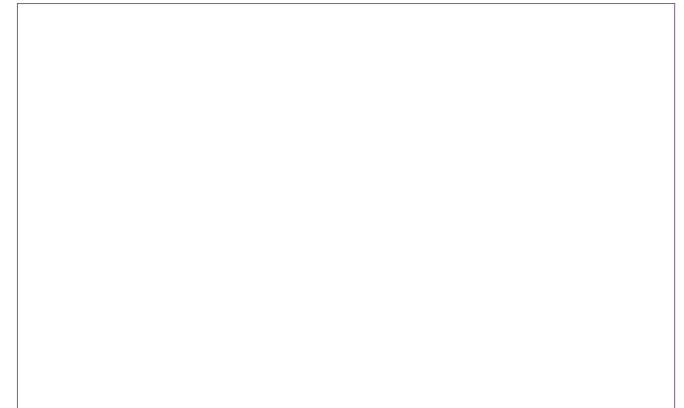
Foundation ○

You have an induction for all incoming academics, visiting or new staff, on campus research security arrangements.

○

Intermediate ○ ○

You run induction and regular refresher training on research security issues, supported by on campus messaging and comms for academic staff including visiting academics.

○

External training

Foundation ○

The university provides relevant information for staff to attend relevant external Trusted Research partner training, including Intellectual Property Office training on knowledge assets and knowledge asset-management and Export Control Joint Unit training.

○

Intermediate ○ ○

Staff are actively encouraged to attend relevant external Trusted Research partner training, including Intellectual Property Office training on knowledge assets and knowledge asset-management, Export Control Joint Unit training.

○

Developed ○ ○ ○

You engage staff with formal/academic training in security and risk management to oversee Trusted Research activities.

○

Environment: institutional risk and collaboration

Environment: institutional risk and collaboration

Sensitive research

Foundation ◉

You have a means of identifying what research you consider sensitive across the institution and you put in place appropriate protections.

Intermediate ◉ ◉

You put in place appropriate physical, personnel and cyber protections around more sensitive research.

Developed ◉ ◉ ◉

You have a central record of all sensitive research being conducted at your institution which is protected and subject to regular review. You also run lessons learned exercises on the measures in place around sensitive research, applying those lessons across your whole sensitive research stable where applicable.

Risk review

Foundation ◉

You have a risk register, and a process to review collaborations according to university risk appetite.

Intermediate ◉ ◉

You have a scheduled review period for high risk research collaborations built into the written agreements from the start. High risk collaboration contracts are regularly reviewed by the team or roles responsible for Trusted Research risk.

Developed ◉ ◉ ◉

Review cases are published with institutional lessons learned, and used to workshop Trusted Research practice across the sector.

Recording

	Intermediate ○ ○	Developed ○ ○ ○
	You have an accessible register and record of funding and funders for all research projects. ○	You can evidence that staff actively manage and record risks as part of research collaborations from the start. ○
	Data on all formal research collaborations are recorded (parties involved, terms of collaborations) and are centrally retrievable. ○	Concerns which have led to changes in risk assessment or lessons learned are reviewed and published for the benefit of others. ○

Recruitment

Foundation ○

You have relevant policies on pre-employment checks, which identify security concerns.

Intermediate ○ ○

Security considerations are written into recruitment policies and employment contracts, aligning with institutional risk appetite.

Developed ○ ○ ○

Trusted Research compliance is advertised as a positive way of working in recruitment material.

Policies on visitors

Foundation ○

You have relevant policies for visitors, covering access to buildings and facilities, IT and ensuring valid visa status where necessary. These policies include additional provisions for those from 'high-risk' jurisdictions (as defined by your institutional risk matrix).

Employment contracts and policies

Foundation ⊙

You have relevant policies for any incoming academic staff, whether permanent or otherwise (including secondees), covering access to buildings and facilities, IT and ensuring valid visa status where necessary. These policies include additional provisions for those from 'high-risk' jurisdictions (as defined by your institutional risk matrix), and the ability to address conflicts of interest if they arise.

Intermediate ⊙ ⊙

You have specific policies on conflicts of interest, including how to recognise and manage them, setting out responsibilities.

Developed ⊙ ⊙ ⊙

Employment contracts and agreements covering non-permanent staff (including secondees) contain institutional protection on conflicts of interest and clarifies ownership of knowledge assets and research developed while employed at or attached to the institution.

Environment: institutional risk and collaboration

Policies on secondments out (working overseas)

Foundation ⦾

You have policies for staff working overseas, ensuing that they are not creating informal relationships which may be high risk and not captured in the institution's processes.

Intermediate ⦾ ⦾

Trusted Research concerns are written into your policies around external secondments and outside appointments where appropriate, expressly clarifying university ownership of IP.

Developed ⦾ ⦾ ⦾

All staff working with a high-risk overseas jurisdiction (as defined by your institutional risk matrix) are briefed on legislative and geopolitical risks in those locations.

Overseas travel

Foundation ⦾

You have policies on staff travelling overseas covering access, sharing of material and information, conference attendance, and duty of care.

Intermediate ⦾ ⦾

You have and actively publicise internal guidance on how to manage the risks associated with overseas travel, including export control considerations. You actively link to relevant Export Control Joint Unit resources and the Trusted Research 'Countries and Conferences' guidance.
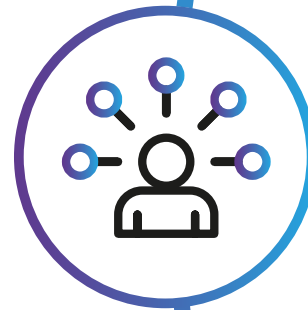
Developed ⦾ ⦾ ⦾

You have an institutional travel risk assessment, identifying institutional priorities for travel and with policies covering different jurisdictions.

Enable: people, processes and guidance

Enable: people, processes and guidance

Staff on campus

Foundation ○	**Intermediate** ○ ○	
You have a process for staff to record and report issues and concerns around high-risk collaborations. Action is taken to address individual issues.	Issues and concerns are centrally reviewed and moderated alongside institutional risk processes.	
○	○	

Response

Foundation ○	**Intermediate** ○ ○	**Developed** ○ ○ ○
You have processes to deal with non-compliance with principles, including stopping collaborations where mitigations do not reduce the risk to an acceptable level.	You can demonstrate that you have intervened in cases where research risk is unacceptable, giving examples of mitigated risks and lessons learned.	You publish case studies of risks mitigated by your institution to educate other institutions.
○	○	○

Due diligence

Foundation ◐

Due diligence is a regularly reviewed internal process for high-risk collaborations, including processes to identify potential non-compliance at the earliest possible stage.

◯

Intermediate ◐ ◐

Your due diligence processes extend to research funders and sponsored positions, considering financial exposure and issues which might arise from allowing high-risk entities to fund sensitive research or specific positions within your institution.

◯

Developed ◐ ◐ ◐

You have a process for identifying risks associated with new collaboration partners who join part way through a collaboration. You seek agreement from funding partners for new partners joining existing collaborations. You comply with UKRI funding terms and conditions particularly RGC 2.6.2.

◯

Entry and exit procedures

Foundation ◐

Entry and exit procedures are in place and established in organisational policies and processes, with staff reminded of their enduring obligations to the university and ownership of knowledge assets/ research and. Staff check what material, if any, they intend to retain upon exit.

◯

Enable: people, processes and guidance

High risk jurisdictions

Foundation ○

You have a process for identifying travel and contact with high-risk jurisdictions.

Intermediate ○ ○

Staff travelling to high-risk jurisdictions receive a briefing on the security situations, FCDO advice and legislative risks.

Developed ○ ○ ○

You publish your own institution's assessment on high risk jurisdictions, with specific guidance on how to work in them.

Reporting concerns

Foundation ○

You have procedures for staff reporting Trusted Research-relevant concerns when overseas.

Intermediate ○ ○

Concerns are centrally recorded, and regularly assessed, feeding into institutional risk assessment.

Developed ○ ○ ○

Concerns which have led to changes in risk assessment or lessons learned are reviewed and published for the benefit of others, but not to the detriment of information protection where relevant.

Environment: data and devices

Leadership

Foundation ○

The board are briefed on, and endorse, the cyber security approach chosen to protect the most sensitive research. Ownership of cyber security at board level is agreed.

Intermediate ○ ○

The board are regularly briefed on the cyber security approach. The board ensure that there are suitably qualified and experienced staff to deliver the chosen approach.

Developed ○ ○ ○

Organisational plans are developed with a full understanding of the cyber security implications. All aspects of cyber security are regularly reviewed and endorsed by the board.

Risk Management

Foundation ○

You have chosen, agreed and implemented a cyber risk management approach for the most sensitive research. You have chosen and implemented a set of baseline cyber security controls or simple standards (such as Cyber Essentials) to protect the most sensitive research.

Intermediate ○ ○

Exceptions to the baseline controls are actively monitored and managed. Risk assessments for sensitive research are carried out and the results are implemented.

Developed ○ ○ ○

Risk management of the most sensitive research is ongoing and is updated regularly in response to changes in the organisational context, changing threats and vulnerabilities.

Environment: data and devices

Improve

Foundation ○

You have an agreed plan to improve the cyber security of your most sensitive research. You monitor and report on progress against this plan to business leaders.

Intermediate ○ ○

The plan is adopted across all relevant areas of the organisation and is funded and resourced sufficiently to achieve its aims.

Developed ○ ○ ○

The plan is regularly reviewed to ensure it is achievable and is updated to reflect changes in business priorities.

Test

Foundation ○

You have an agreed plan to test the cyber security of the most sensitive research.

Intermediate ○ ○

The plan includes a mixture of process and technical testing to provide confidence in the cyber security of the most sensitive research.
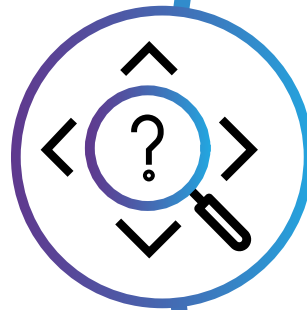
Developed ○ ○ ○

The plan is regularly reviewed to ensure it tests the areas of largest risk, and is conducted by appropriately skilled experts, including bringing in outside expertise when necessary.
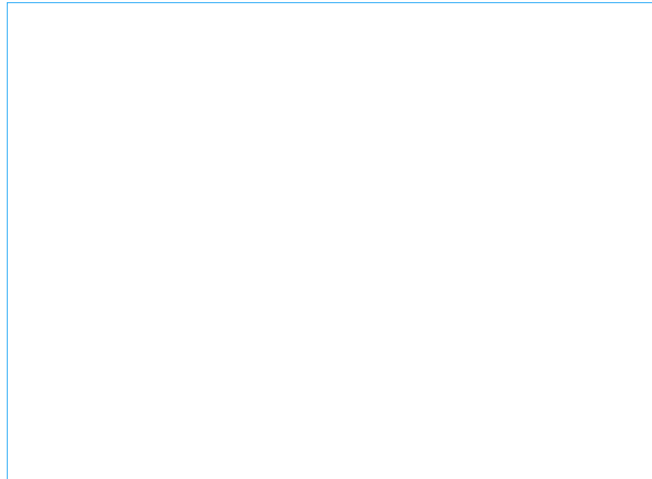
Evaluate: impact measurement

Evaluate: impact measurement

Governance/endorse

Foundation ○

You can evidence board-level discussions around security topics through minutes/meeting records.

○

Developed ○ ○ ○

You can evidence the referral of high-risk collaborations for internal decision making and maintain a risk register of all collaborations including details of mitigations placed on collaborations and decision making around whether to proceed.

○

Comms/encourage

Foundation ○

You collect statistics and metrics of staff engagement with your research security comms.

○

Intermediate ○ ○

You conduct an annual survey of academic research staff in STEM areas and have an awareness of Trusted Research and staff responsibilities in relation to university policies on research security.

○

Developed ○ ○ ○

You can evidence that over 80% of academic research staff in STEM areas are aware of Trusted Research and clear on their responsibilities and the institution's policies.

○

Environment

Foundation ○

You record and can evidence engagement with RCAT and any other relevant oversight bodies.

○

Intermediate ○ ○

You collect statistics and metrics on your collaborations and can provide thematic breakdowns according to security concerns.

○

Developed ○ ○ ○

You use outputs from collected information on how security issues manifest in your institution to shape action and engagement.

○

You can evidence the referral of export control licence applications and end user checks.

○

Disclaimer

This framework has been prepared by NPSA and NCSC and is intended to help academic institutions self-assess their level of research security maturity. This document is provided on an information basis only, and whilst NPSA and NCSC have used all reasonable care in producing it, NPSA and NCSC provide no warranty as to its accuracy or completeness.

It is important to emphasise that no security measures are proof against all threats. You remain entirely responsible for the security of your own sites and/or business and compliance with any applicable law and regulations and must use your own judgement as to whether and how to implement our recommendations, seeking your own legal/professional advice as required.

To the fullest extent permitted by law, NPSA and NCSC accept no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using the Trusted Research Evaluation Framework.

This exclusion applies to all losses and damages whether arising in contract, tort, by statute or otherwise including where it is a result of negligence. NPSA separately and expressly exclude any liability for any special, indirect and/or consequential losses, including any loss of or damage to business, market share; reputation, profits or goodwill and/or costs of dealing with regulators and fines from regulators.

Institutions and individuals have a responsibility to ensure that they comply with all relevant legal obligations, as well as any other obligations to which they are beholden. This framework and the mitigations included in this document should not be considered exhaustive. This framework raises issues for consideration but does not dictate or purport to dictate what conclusions institutions should reach.