MANAGING RISKS IN INTERNATIONALISATION: SECURITY RELATED ISSUES

Universities UK

CONTENTS

Key definitions 3

Foreword 4

Summary 6

Overview 10

1: Protecting your reputation and values 13

1.1: Building resilience to security-related issues 14

1.2: Due diligence 18

1.3: Promoting the values of UK higher education 23

2: Protecting your people 27

2.1: Internal and external communications and knowledge-sharing 28

2.2: Protecting staff and students travelling and working overseas 31

3: Protecting your campuses 34

3.1: Cybersecurity, estates and visitors 35

4: Protecting your partnerships 40

4.1: Research security, intellectual property and export control compliance 41

4.2: Transnational education partnerships 44

Forward look 48

Glossary 49

Annex 1: Summary of resources available to institutions 51

Annex 2: Guiding questions for cybersecurity, estates and visitor policies 55

Annex 3: Checklists for research security, intellectual property and export controls 56

References 58

KEY DEFINITIONS

internationalisation: the term 'internationalisation', as applied to higher education, is broad. In the context of these guidelines, internationalisation describes the purposeful integration of international and intercultural dimensions into aspects of university activity.[1]

security-related issues: the term 'security-related' is an umbrella term that describes a broad range of issues and risks that are associated with internationalisation. The security-related risks referred to in these guidelines can be broadly grouped into two categories: attempts by overseas/hostile/external actors or those acting on their behalf to illegitimately acquire academic research and expertise; and/or interfere with academic discourse. Universities must manage security-related issues and risks. If left unmanaged, these risks may impact reputation and values; people; campuses; and education and research partnerships of the UK HE sector.

Other significant terms are described in the Glossary.

[1] https://link.springer.com/chapter/10.1007/978-3-319-20877-0_5

FOREWORD

Professor Sir Peter Gregson and Professor Anthony Finkelstein

Internationalisation has shaped the agenda and strategies of universities not just in the UK, but globally. It has brought significant economic and social benefits to the UK, and intellectual opportunities for scholarship, while transforming universities into global institutions. The UK benefits from international research collaborations. Collaborations with international partners continue to be vital to the continued success of the UK's research and innovation sector. The UK's universities are world-leading, but they do not have a monopoly on brilliant researchers, and the UK benefits from the skills and expertise of researchers based at research organisations overseas.

The sector has historically done a good job of managing the risks associated with internationalisation. However, the risks are increasingly dynamic and growing in complexity. In this context, institutions will need to review and adapt their risk management processes.

These guidelines are intended to support universities, enabling them to protect themselves, their staff and students, and to manage risks associated with internationalisation, amid intensified international strategic competition, political polarisation and backlash against globalisation. These risks, as outlined below and throughout this document, are faced by all universities, and every university should have a plan in place to protect the society of which it is a part, its reputation and its values, people, campuses and partnerships.

The guidelines are designed to provide the governing body and the executive head of the university with the tools and the support needed to manage these risks. The university should necessarily draw on academic and professional expertise; however, accountability rests with the governing body and the executive head of the institution.

Although this is the first time Universities UK (UUK) has produced guidelines on this subject, the risks described here are not a new phenomenon. Universities are not starting from a zero base and have developed governance and risk management processes in place to protect individuals, institutions, and the sector. What has changed is the dynamism of the threat landscape and the centrality of universities, science and technology to the future security and prosperity of the UK. As their role and significance increase, universities become more valuable targets. Senior leaders must be aware of the risks and ensure that all members of their community are aware of their own roles and responsibilities in this regard.

The risks to universities are not limited to the theft of intellectual property and data, or the security of university campuses. There are also threats to the values that have underpinned the success of the higher education sector: academic freedom, freedom of speech and institutional autonomy. These values are rooted in the UK's commitment to democracy and the rule of law.

There is increasing awareness of the potential impact of these threats. In the last couple of months, attempts to access UK-based research related to Covid-19 (coronavirus) have been widely reported. The Australian National University has released a report into the impact of a data breach that took place in late 2018, which was the consequence of a successful and sophisticated cyber-attack. Other threats are less well-defined and understood, but a re clearly in evidence, such as activities intended to interfere with or undermine the values that underpin the success of the UK's universities. Taking teaching online due to the Covid-19 crisis has presented new risks to the security of students and academic staff due to uncertainties over access to personal data and the unwarranted monitoring of learning activities.

The UK's universities have always been a crucible for debate, covering both domestic and international issues, many of which have been or continue to be contentious. It is critically important that universities continue to play this role, providing the space for such debates to take place.

These guidelines are not intended to inhibit a bold and outward-looking higher education sector. Rather, UUK is seeking to equip universities with the tools to pursue their goals in a clear-sighted and risk-managed manner.

These guidelines are intended to complement the existing information, advice and guidance available to institutions, such as the Trusted Research campaign developed by the government authority for protective security advice, the Centre for the Protection of National Infrastructure (CPNI). These guidelines should be read in the wider context of the information available to institutions. Institutions should also make use of the support available from government.

Good governance and effective risk management processes will help to protect individuals, institutions and the sector from the legal, financial and reputational consequences of security-related risks. Without such protections, institutions are likely to suffer from significant reputational and financial ramifications. A proactive approach across the sector, at both an individual and institutional level, will allow institutions to realise the benefits of diverse international research collaboration. The ability of the higher education sector to provide greater assurance on the security of its international research collaborations, will have a positive impact on the prosperity and security of the UK.

In summary, universities have a leading role to play in the future prosperity and security of the UK and sustaining our shared values. These guidelines will help assure a future for extended international collaboration, safeguarding the excellence of the sector.

SUMMARY

This summary provides an overview of the key messages and actions of these guidelines.

Overview

The governing body and executive leadership of the institution are responsible and accountable for protecting the institution against the threats and risks set out in these guidelines. To support them in performing this role, the governing body of the institution should receive an annual report describing the risks the institution faces and how the risks are being mitigated.

Structure of the guidelines

The guidelines are divided into four chapters:

- **1: Protecting your reputation and values** – governance, processes and policies
- **2: Protecting your people** – roles and responsibilities of those working or studying at the institution, measures to protect staff, students, and visitors and the risks of online contact
- **3: Protecting your campuses** – cybersecurity and UK campuses
- **4: Protecting your partnerships** – research security and transnational education.

The chapters are divided into thematic areas (see Table 1).

Table 1: Structure of these guidelines

Chapter	Thematic areas
1: Protecting your reputation and values	1.1 Building resilience to security-related issues 1.2 Due diligence 1.3 Promoting the values of UK higher education
2: Protecting your people	2.1 Internal and external communications and knowledge-sharing 2.2 Protecting staff and students travelling and working overseas
3: Protecting your campuses	3.1 Cybersecurity, estates and visitors
4: Protecting your partnerships	4.1 Research security, intellectual property and export control compliance 4.2 Transnational education partnerships

1: Protecting your reputation and values

1.1: Building resilience to security-related issues [p14]

Your institution's risk exposure is unique and depends on a range of factors. It will change over time as your institution and the environment change.

Establish security-related risk management as a key, ongoing priority. This should include:

- aligning policies and processes with your institution's risk profile
- supporting and empowering individuals to identify and report security-related risks
- regularly reviewing risk frameworks to ensure that they are fit for purpose and in line with best practice.

1.2: Due diligence [p18]

Your institution will have due diligence processes in place, but it is likely that these will have been primarily focused on financial and reputational risks. Your institution should look again at due diligence processes and ensure that:

- you consider reputational, ethical and security risks in your formal processes
- your institution is making good use of publicly available information, including information from the government
- you are building and sustaining a culture that enables staff to raise concerns about potential or current partnerships
- current and prospective partners are aware of your institution's commitment to academic freedom and freedom of speech, and the implications for working in collaboration.

1.3: Promoting the values of UK higher education [p23]

Rigorous, informed debate is the foundation of high-quality higher education and the advancement of knowledge.

To identify and manage the risks of interference, you should:

- develop and promote clear codes of conduct, policies and legal agreements that enshrine the core values of academic freedom and freedom of speech
- promote open and transparent communication, debate, research and enquiry about what interference might look like
- support staff and students to take responsibility for protecting against these infringements throughout their engagements and activities
- develop processes and mechanisms through which staff and students can report any concerns and receive support in relation to issues connected to academic freedom and freedom of speech.

2: Protecting your people

2.1: Internal and external communications and knowledge-sharing [p28]

Institutional policies and processes will help protect your institution, but they will not be effective without a culture of awareness, in which individuals understand their responsibilities to identify, report and manage security-related risks.

You should promote transparency, and in doing so, build confidence in your institution's ability to undertake mutually beneficial international collaborations.

2.2: Protecting staff and students travelling and working overseas [p31]

Students and staff who are travelling in the course of their work and study may be exposed to specific, and in some cases severe, personal risks.

Your institution should have processes in place that are proportionate and applied to all international travel. This should include adequate training for students and staff that ensures they understand the relevant policies and codes of conduct, and supports them to self-manage their risk.

3: Protecting your campuses

3.1: Cybersecurity, estates and visitors [p35]

The UK's universities are proudly dynamic, diverse and international institutions, bringing together staff, students and visitors from across the globe throughout the year. Institutions play an important civic role, supporting their communities and providing communal and open spaces.

Your institution should balance this civic role with the need to protect your institution and its assets. You should develop integrated estates and visitor policies and ensure that cybersecurity strategies are developed and implemented.

4: Protecting your partnerships

4.1: Research security, intellectual property and export control compliance [p41]

The UK's world-leading research is increasingly open and collaborative. This is fundamental to the UK's success, but presents risks and challenges. Universities are subject to targeted attempts by individuals and organisations to improperly gain access to research and intellectual property (IP).

Your institution should be aware of the key security threats and challenges and take action to mitigate the risks by ensuring that your institution:

- conducts proportionate due diligence on all prospective overseas partners, for all types of collaboration
- implements policies and contractual agreements to protect IP
- complies with export control legislation for controlled technologies, and other legal requirements.

4.2: Transnational education partnerships [p44]

UK universities hold a reputation as world leaders in transnational education (TNE), and there are nearly 700,000 students registered on UK programmes overseas. Transnational education arrangements are subject to local regulations and must comply with instructions from local authorities, a characteristic which brings greater risks.

Your institution should have risk mitigation policies that acknowledge and assess the existence of risks that may affect overseas partners differently. In particular, you should ensure your institution:

- undertakes thorough and regular due diligence on overseas partners
- recognises, within your risk registers and risk statements, risks related to institutional autonomy and academic freedom overseas
- balances requirements for local autonomy with robust, centralised risk management
- establishes clear reporting lines for communication with local stakeholders
- develops an exit strategy that is supported by a comprehensive, rules-based arrangement and high-level principles.

Additional resources

A wide range of resources have been developed to support your institution and your colleagues to understand and manage the risks identified in these guidelines. There are further resources in development, including on cybersecurity, export controls and protecting academic freedom. These guidelines will be periodically updated as and when these additional resources become available.

The Centre for Protection of National Infrastructure (CPNI) and the National Cyber Security Centre (NCSC) have published material that will support institutions to make decisions and mitigate risk, including Trusted Research[2]. These resources are identified in the relevant sections of the guidelines. A list of all resources mentioned appears in the References at the end of these guidelines.

[2] www.cpni.gov.uk/trusted-research

OVERVIEW

How to use these guidelines

Implementation of these guidelines will require buy-in from every member of the university community, but the responsibility for protecting your institution against the risks and threats set out in these guidelines cannot be delegated. The governing body and senior leadership team must establish a clear governance structure, identifying the staff members who will be responsible for managing the risks set out in these guidelines. The senior leadership team should provide the governing body with the appropriate assurance that the institution has an effective set of arrangements in place that are operating properly. This is likely to include transformational and cultural change, as well as changes to institutional systems, processes and policies.

We strongly recommend that the governing body of the institution receives an annual report on how the institution is managing security-related risks associated with internationalisation, describing the risks faced by the institution and how the risks are being mitigated. This should provide an overview of the systems and processes that are in place to manage security-related risks, while also protecting institutional autonomy and academic freedom, as well as information that sets out how the institution is raising awareness of these issues among the staff and student body of the institution.

Purpose of UUK's work

Universities UK (UUK) has established a programme of work on security-related issues in higher education to realise three long-term goals:

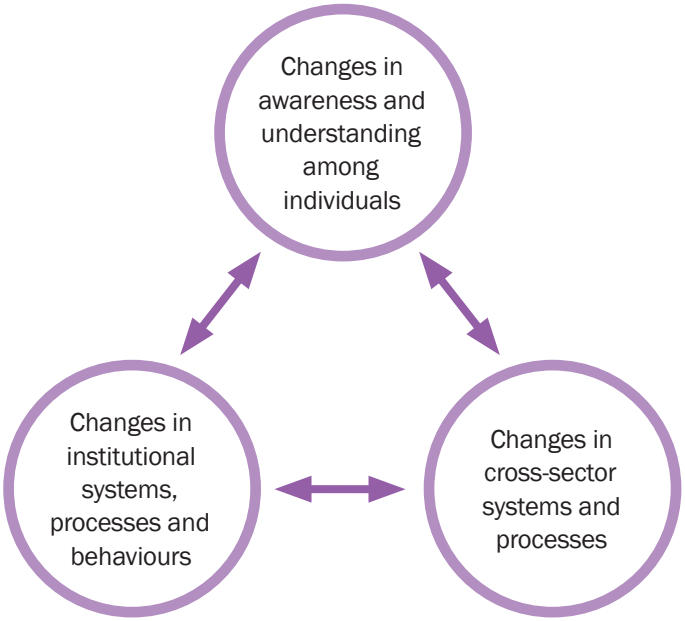
1. UK universities can demonstrate that they have coherent, proactive, strategic, and operational approaches to managing and mitigating international security threats.
2. UK universities are confident and able to pursue sustainable, secure international partnerships.
3. The UK higher education sector and the government have a clear, collaborative and constructive approach towards protecting and promoting growth in research and innovation (R&I), institutional autonomy and academic freedom in the context of security challenges.

To achieve these goals, UUK has identified three intermediate outcomes:

- increased awareness and understanding among individuals, both staff and students, of security-related issues
- stronger institutional systems, processes and behaviours,
- wider changes to the ecosystem including the interface between universities and government, and in the resilience of the system.

These intermediate outcomes overlap with each other and are mutually reinforcing.

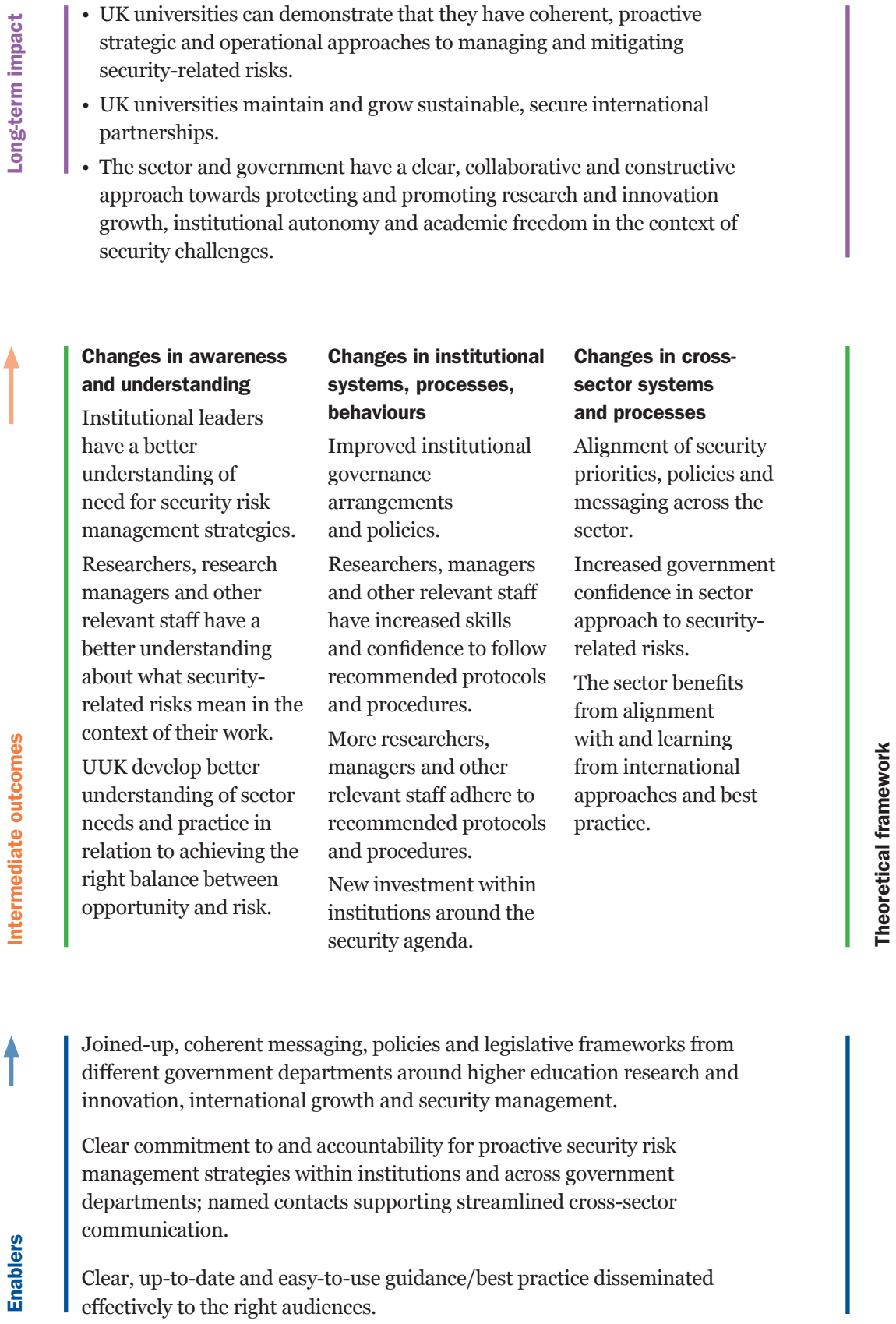
Figure 1: Intermediate outcomes of the UUK's approach to security-related issues



The purpose of these guidelines is to support institutions in making progress towards the first two outcomes. Through the use and distribution of these guidelines, we believe that there will be an increase in awareness and understanding of the issues that these guidelines cover. In turn, this will lead to changes in systems, processes and behaviours. These changes will benefit your international collaborations and the security, prosperity and continued success of your institution. Although UUK and the government have enabling roles in this, it is ultimately up to individual institutions to make sure they use the information, advice and guidance available to them to inform and drive change.

The changes required to the wider ecosystem of the sector, including in the interface between universities and government, is important, but isn't directly addressed in these guidelines. The government and higher education sector are working together to ensure that the wider ecosystem supports universities to meet the challenges set out in this publication. The risks considered in these guidelines are both dynamic and complex. The debates and discussions around the issues considered in this set of guidelines are ongoing, and more support, including advice and guidance will be made available to institutions in due course. To support those ongoing discussions, we encourage users of the guidelines to contact UUK if they wish to contribute to this wider set of conversations, particularly if they have identified perverse incentives or other issues that might hinder, rather than help, individuals and institutions to respond to the issues covered by these guidelines.

Figure 2: UUK programme of work



1
PROTECTING YOUR REPUTATION AND VALUES

Overview

The success of your institution depends on its reputation, and the success of the UK's universities is underpinned by the reputation of the UK higher education sector, and its shared values of academic freedom, freedom of speech and institutional autonomy.

This chapter is intended to support your institution in protecting its reputation and the values that underpin the success of the UK higher education sector. As a senior leader, your risk awareness will be more developed than that of many others in your institution. Your visible endorsement of a secure approach to international collaboration is vital to successful implementation and compliance across your institution.

Much will rest on institutional resilience to security-related issues. This chapter details how institutional resilience can be strengthened by:

- developing a positive, risk-informed culture, underpinned by robust governance, reporting and risk-management structures
- incorporating security-related issues into due diligence procedures, particularly so as to secure a comprehensive understanding of the UK's legislative and regulatory requirements when forming international agreements and partnerships
- securing clear policies and processes that build a culture of collective responsibility for upholding the values of academic freedom, freedom of speech and institutional autonomy, as well as the protection of students and staff.

The audit committee of your governing body should include a standing item on security related risks on its risk register.

1.1: Building resilience to security-related issues

Develop a risk-literate, risk-aware culture

Senior leaders improve institutional resilience to security-related issues by prioritising the development of a positive, risk-literate, risk-aware culture and implementing clear governance, reporting and risk-management structures that promote the strengths and values of UK higher education.

There are steps senior leadership teams should take to facilitate successful international collaborations, while ensuring that exposure to security-related risks are identified and managed. This is a strategic priority for senior leaders of higher education institutions.

As leaders, you are highly skilled in risk management and invest significantly in the development and maintenance of due diligence, governance and reporting processes to ensure international collaborations are of the highest quality.

While the vast majority of international collaborations are welcome and mutually beneficial, it is essential that you remain alert to activities that may threaten the security and standing of your institution. These activities include the targeting of institutions such as yours to obtain sensitive information, suppress or manipulate academic freedoms, and exploit the excellence of the UK higher education sector. These activities have financial, legal and reputational consequences for those institutions and individuals involved. Accordingly, it is essential for your institution's continued success – and for the security and prosperity of the UK – that you understand your institution's exposure to these risks and prioritise its protection.

In the development of these guidelines, senior leaders at UK institutions highlighted key challenges that prevent or hinder the effective management of security-related risks:

- incomplete understanding among senior leadership teams and key individuals of the nature and scale of security-related risks, and their responsibilities to manage them
- institutional cultures where staff may be unaware of the risks or not sufficiently empowered to act on the risks that they have identified within the risk-management processes
- risk-management, governance and reporting processes that are not regularly updated or equipped to respond to the changing nature of these risks.

Identify and manage exposure to security-related risks

Your institution's risk exposure is unique and depends on a range of factors, including the nature and scope of your activity, and the risk awareness and management culture you have fostered. Your risk exposure will change over time.

Failure to manage security-related risks may result in serious consequences – financial, legal, and reputational. In some cases, consequences may be felt beyond your institution and affect the national security and prosperity of the UK.

Non-compliance with relevant legislation and regulations, and contractual arrangements, including export controls, the Academic Technology Approval Scheme (ATAS) and General Data Protection Regulation (GDPR), may expose you, your institution or individuals within your institution to criminal charges or litigation. The nature and terms of your collaborations and duties of care, as well as the information individuals have access to, will give rise to specific and evolving legal obligations. Classified research materials, for example, are subject to specific and enforceable handling requirements.[3] Where collaborations include overseas activity, you may be subject to local legislation and regulations.

Consequences may result from individual risks or as a result of cumulative risk. As a senior leader, you are one of the few people in your institution appropriately placed to identify cumulative risk exposure, and, with your governing body, determine your institution's risk profile. Accordingly, you must consider where the combined effect of investments and activities may create an environment in which your institution is exposed to undue external leverage.

International collaborations are fundamental to the academic, reputational and financial success and sustainability of UK universities. However, there are potential adverse and long-term implications of, for example, undertaking non-secure research collaborations. This may render your institution unable to attract future funding or realise the commercial or financial benefits of innovation because research, data or other materials have been stolen, compromised or used in contravention of national and international agreements.[4] Joint research is particularly vulnerable to misuse by organisations and institutions that operate in other countries.

[3] Further information on export controls is set out in Section 4.1.

[4] Theft could occur systematically over a prolonged period of time, rather than as a one-off event.

Reputational damage may result from the improper management of security-related risks and affect your institution's ability to maintain high-quality provision and attract and/or retain funding, students, staff and accreditation.

In short, you should proactively consider security-related risks that have the potential to affect your institution's standing and the UK's security and prosperity.

The descriptions above are not exhaustive and additional information can be found in the following sections:

- Cybersecurity, estates and visitors (see Section 3.1)
- Research security, intellectual property and export control compliance (see Section 4.1)
- Protecting staff and students travelling and working overseas (see Section 2.2)

Your institution is not alone in facing these risks. Knowledge-sharing and engagement, including instances in which engagement is required by law, are covered in more detail under internal and external communications (see Section 2.1).

Establish security-related risk management as a key, ongoing priority

Your institution will have a range of risk-management, governance and reporting frameworks and capabilities in place to manage risk. Risks, including those related to academic freedom and freedom of speech, should be covered in these processes and publicised widely across your institution.

A shared understanding of the policies and processes in place to manage these risks, including individual responsibilities to proactively report and escalate security-related risks, is crucial to fostering a culture of awareness and security and is discussed further under internal and external communications (see Section 2.1).

Policies and processes must align with your institution's risk profile. A higher risk profile may necessitate more robust due diligence processes and oversight and subject your institution to additional scrutiny. Assessment of your risk profile must be informed by a robust understanding of your legal obligations.

It is vital that individuals within your institution feel able and supported to identify security-related risks, without fear of retribution or censorship. Institutions should have in place appropriate policies and processes so that staff know how to report issues or concerns. This may be especially contentious where it is perceived to intersect with religious, national, racial or social identities or is conflated with prejudice or racism. Despite this, institutions will need to address these issues, ensuring that appropriate policies and processes are in place.

These risks are dynamic. As the threats evolve, so too should the systems and processes in place to manage them. Risk frameworks should be regularly reviewed to ensure they are fit for purpose and in line with best practice. In certain circumstances, independent organisations may need to provide assurance of the controls in place.

Case study: Governance

The case studies in these guidelines are hypothetical, and they are intended to support the user to apply these guidelines in practice.

The senior leadership team at a UK higher education institution requested a review of its institution's governance processes for international collaborations. The review was in response to an increase in the scale, scope and variety of the institution's international partnerships and sought to identify policies that would facilitate safe and sustainable partnerships.

As a result of the review, 'significant international collaborations or partnerships' required explicit authorisation from the vice-chancellor, including:

- any project that may result in the establishment of a joint campus or representation of the institution overseas
- any venture or entity wholly or partially funded by international partners
- any project requiring staff to be based overseas for extended periods
- any project with novel or contentious characteristics that could involve reputational, security or legal risks, irrespective of monetary value.

To assist the vice-chancellor, an international group was formed, chaired by the deputy vice-chancellor international and comprising relevant professional services and senior academic staff. This policy change was communicated across the institution.

The scenario

A collaboration opportunity was presented to the international group. Academics from the institution were invited to travel to an overseas university, deliver a series of guest lectures on their area of expertise (plant biology) and provide generic advice on establishing research facilities. Their travel and accommodation costs would be fully covered by the international partners, but they would not receive any further compensation.

The international group had initial reservations about this collaboration. Web searches relating to the overseas university returned limited results and its representatives, although forthcoming in their disclosures, had been sporadic in their contact. Further enquiries, including contact with an overseas embassy, revealed that the proposed partner institution had been established for a year and had reached out to a number of UK and other international institutions and organisations for assistance and collaboration. A number of these collaborations had taken place without issue.

The international group determined that, with appropriate safeguards in place, the project was a promising opportunity. Despite not being financially lucrative to the university, the partner country would benefit from being able to improve local farming techniques and allow the university to develop a presence in an overseas market and could attract additional investment opportunities.

Following consideration of relevant advice, the UK institution ensured that:

- travelling academics only took and had access to the information they needed while travelling, with safeguards in place so that they were temporarily unable to access collaborative datasets and their institution's intranet while outside the UK
- planned advice relating to research facilities was generic and high level, and not in conflict with the UK's strategic export controls

- the academics understood they were not to accept any further gifts or offers from the overseas institution, and advised on how best to decline offers in a culturally sensitive manner, so as to not offend their hosts
- legal advice was sought before the trip, which found no problem with the collaboration agreement, but identified that virtual private networks (VPNs) were illegal in the overseas country, and recommended further input from cybersecurity colleagues.

The collaboration went ahead without issue. Although there has been limited engagement since the visit, the academics found the trip useful and have recommended the international group as a useful and necessary service to colleagues.

Additional resources on resilience

- CPNI *Trusted Research: Guidance for senior leaders* available at: www.cpni.gov.uk/system/files/Trusted%20Research%20Guidance%20for%20Senior%20Leaders.pdf

1.2: Due diligence

Productive international collaborations are fundamental to the success of the UK higher education sector and its reputation for quality, diversity and impact. While most international partnerships benefit all parties, there will be a small number of cases where there are significant risks. In some instances, parties may engage in bad faith, seek benefits beyond the terms of the agreement or extend activity beyond that set out in the agreement. Accordingly, robust due diligence, which is subject to regular review, is essential to facilitate strong, successful, mutually beneficial international partnerships, and to minimise harm to institutions, the sector and the interests of the UK.

Senior management should provide assurances to the institution's governing body that security-related issues are fully incorporated into due diligence, to promote a comprehensive understanding of the partnership and awareness of legislative and regulatory requirements in the UK and any other countries involved.

The UK's universities regularly conduct due diligence on prospective partners. To date, this activity has primarily focused on financial and reputational risk. We encourage institutions to look again at their existing due diligence processes, with consideration of the government's and other guidance and to consider the efficacy of their due diligence processes and how they assess reputational, ethical and security risks.

Universities are autonomous institutions, and it is up to individual universities to determine how best to mitigate risks, in accordance with the relevant legislation and regulations, as well as what an appropriate level of risk is. This assessment should be proportionate and is likely to be informed by the scale and nature of the planned collaboration and the location and the status of the partner.

This section provides information and guidance that will help institutions to develop due diligence processes that assess the security-related risks and mitigate potential damage to the institution. The section is divided into three parts: know your partner; strike and maintain robust agreements; and establish a clear set of roles and responsibilities for staff.

Know your partner

UK universities have a complex network of international engagement, ranging from informal collaborations, such as dialogue and co-operation between individual staff to formal partnerships, including transnational education. Some of these collaborations will expose the institution to security-related threats. These collaborations are necessarily shaped by the countries in which partners are based. As a result, governance and due diligence should be tailored accordingly. For example, public records may be limited in some jurisdictions, and it might not be possible to obtain detailed records.

Although informal collaborations are unlikely to be covered by the institution's formal policies or procedures, risks remain. Your institution should consider how it supports staff to make informed decisions outside your formal policies and procedures, including requiring staff to disclose partnerships and collaborations wherever possible. This will ensure that your institution has visibility of any conflicts of interest and other legal, reputational or financial risks associated with informal collaborations.

Make risk-informed decisions

How does your institution support academics to make informed decisions outside formal due diligence processes? For more formal partnerships with an international university, company or government agency, due diligence must include enquiry into the partner's past activities, the sector it operates in, as well as the commercial and ethical standing of its governing body, and the legal and regulatory environment of the proposed partner.

Universities typically ask partner organisations to complete a questionnaire or submit documentation or evidence that is then used to assess the level of risk involved in working with the partner. Universities also make use of the academic experts employed at their institution, web searches, subscription services and professional firms. How does your institution use publicly available information to enhance its understanding of partners, their links to other activities or states, and the legislative context in which they operate? To what extent is your institution able to undertake or commission background checks on prospective partners and their employees, in the same way major businesses in the private sector would?

In any partnership, the risks depend to a significant extent on the collaborative activity being proposed. Some activities are covered by specific legislation, regulations and codes of conduct, such as the Academic Technology Approval Scheme (ATAS) or export control legislation.[5] Do your institutional risk management frameworks recognise and respond to relevant legislation, regulations and codes of conduct? To what extent is your institution drawing on the advice and expertise of the UK Government to make decisions?

Strike and maintain robust agreements

Due diligence on prospective international partners should be proportionate and reference relevant legal and regulatory provisions. It should include consideration of all security-related risks, including any risks to academic freedom that are associated with international partnerships. Be clear about monitoring data, and who is responsible for reporting what to whom.

---

[5] For further information on ATAS or export control legislation, please consult Section 4.1, particularly the additional resources.

For all formal interactions with partner organisations or individuals, use best practice contracting mechanisms and policies to manage security-related risks. Terms and conditions of agreements or memoranda of understanding should include clauses that protect the integrity of academic activity.

Internal stakeholders, including professional services staff, benefit from training and awareness sessions and from simple risk assessment tools to manage engagement activity, including visits and delegations.

Due diligence to mitigate security-related risks should be undertaken regularly, with regular reviews in relation to international partnerships and projects, including research partnerships, as well as sources of income, such as investments, donations, philanthropy, commercialisation, capital investment, tuition fee income and staff honorary and consultancy appointments. Full consideration should be given to the potential for security breaches in every engagement, from the most informal collaboration to the most formal partnership.

The UK institution should have in place an appropriate exit strategy with provisions in place, along with an understanding of what would trigger an exit. Ultimately, this could include the right to withdraw from the agreement or terminate it early without incurring any liabilities if the ongoing due diligence exercise reveals that the overseas organisation or researcher is no longer an appropriate partner. An example would be where the ongoing due diligence exercise reveals that the university's legal obligation to maintain academic freedom is under threat.

Specific legal advice should be sought in relation to contract design and ensuring the appropriate protections are in place.

Partner organisations or individuals may seek to access or influence particular areas of activity through various forms of funding arrangements and other inducements targeted at individuals. To mitigate this, individuals and institutions should be transparent about their sources of funding. Due diligence should establish which processes exist to manage security-related risks when considering sources of potential income.

Establish clear roles and responsibilities for staff

Universities already have procedures and policies in place to help identify, develop and manage risks associated with international engagements. There is growing awareness of security-related risks, and universities should support staff to identify these risks and to act on them.

Key outcomes

- Ensure that due diligence processes consider reputational, ethical and security risks.
- Use publicly available information to enhance your understanding of partners and their links to other activities or states. Where necessary, seek further information the UK government.
- Build and sustain a culture that enables staff to raise concerns, coupled with processes that enable the institution to consider whether activities raise reputational, ethical and/or security risks.
- Ensure that partners understand the UK institution's commitment to academic freedom and freedom of speech and any potential implications this might have for the collaboration or partnership

Case study: Multi-institution collaborative partnership

The case studies in these guidelines are hypothetical, and they are intended to support the user to apply these guidelines in practice.

Two UK universities sought to work collaboratively on a fundamental research programme. The institutions bid for and were successful in securing funding through a specific UK government funding programme in partnership with a research council. The bidding process involved the international partner in the funding programme partnering the UK universities with two organisations from that country.

The scenario

The understanding in the scientific community about the funding programme is that the international side brings to the table those entities that they have decided should be funded. The UK consortium had assumed that because the grant was approved by the funding programme and the research council that the international entities would be appropriate. As a result, insufficient due diligence was undertaken by the UK collaborating universities.

The programme was supported and subsequently delivered a successful collaborative research programme through to completion, with some of the work being published in research journals.

The universities were alerted to the fact that the programme could have breached export control regulations and, had it not been completed, would have been issued with an end-use notification to suspend the programme. Both university partners had equal responsibility for the lack of due diligence and the potential impact on their reputation and that of the institution.

Lessons learned

- Overseas partners may attempt to access the early development stages of new technology and research before it is subject to export control legislation.
- UK partners in collaborative proposals must all take responsibility for due diligence and ongoing audit, which should be overseen by senior colleagues.
- Robust due diligence is required for all international partnerships and collaborations, including those funded by UKRI, UK research councils and other government departments.
- The situation could have been mitigated by relevant points of contact being appointed in each university to share information with other institutions and government and to own the due diligence and auditing process.

Additional resources on due diligence

- ARMA
  Consolidated Approach to Assurance and Due Diligence project available at:
  https://arma.ac.uk/first-output-from-the-consolidated-approach-to-assurance-and-due-diligence-project/

Due diligence

- CPNI
  Campaign implementation plan available at:
  www.cpni.gov.uk/system/files/Trusted%20Research%20Implementation%20Guide.pdf
- CPNI
  Checklist: Evaluating research proposals available at:
  www.cpni.gov.uk/system/files/Trusted%20Research%20Checklist%20for%20Academia.pdf
- CPNI
  Trusted Research: Guidance for Academia available at:
  www.cpni.gov.uk/trusted-research-guidance-academia

Sources to help identify international collaborations or partnerships that fall into the high-risk category:

- UN Sanctions List
- US export entity control list
- HM Treasury's financial sanctions targets
- Country corruption index
- Human Freedom Index
- World Justice Project Rule of Law Index

Templates and frameworks for due diligence

- Economist Intelligence Unit (EIU) (country overviews and risk briefings)
  https://country.eiu.com/All
- FCDO & DfIT
  Overseas business risks available at:
  https://www.gov.uk/government/collections/overseas-business-risk
- Global Edge (sources of statistical information for countries worldwide)
  https://globaledge.msu.edu/global-insights/by/country

1.3: Promoting the values of UK higher education

Institutions have clear policies and processes that build a culture of collective responsibility for upholding our values of academic freedom, freedom of speech and institutional autonomy.

Rigorous, informed debate is at the foundation of high-quality higher education and the advancement of knowledge, underpinned by values of academic freedom and freedom of speech. We must work together proactively to ensure the key values of UK higher education are understood, protected and championed at every level of the institution.

However, there are a small number of well-documented examples in the public domain of international governments and organisations attempting to interfere overtly or covertly in our universities, and to undermine the reputation of individual universities and the sector as a whole.

Interference and influence

The concepts of 'influence' and 'interference' are significant here.[6] Interference comprises malign activity by another state or those acting on its behalf that is designed to have a detrimental effect on the interests of the UK. This activity can be deceptive, coercive or corruptive. It includes the use of agents of influence, leverage of investments, financial inducement, disinformation and disruptive or malicious cyber-activities.

In the context of the UK higher education sector, interference would include malign activity that is contrary to the values and interests of a UK higher education institution. This might include, for example, attempts to alter course content and curricula. In research, it might include the theft of research outputs or data. In some instances, the subject of the interference may not realise that they are a victim of interference.

All governments, including the UK government, try to influence deliberations on issues of importance to them. These activities, when conducted in an open and transparent manner, are a normal aspect of international relations and diplomacy and can contribute positively to public debate. In the context of the UK higher education sector, influence would include activity that is intended to promote open international collaboration, and the interests of the university. This might include, for example, the hosting of cultural exchanges or mutually beneficial international collaborations or partnerships.

The examples provided above are unambiguous. However, the distinction between interference and influence can be vague. Influence might lead to self-censorship and an environment that appears closed in terms of transparency and accountability to staff. Open, transparent debate within an institution is an effective way to manage these risks.

[6] The definition of influence in this section has been based on the definition used by the Australian University Foreign Interference Taskforce.

To counter interference, which may carry significant institutional risks and adversely affect the security of your institution, senior leaders must consider the risks that are posed to academic freedom, freedom of speech and institutional autonomy and promote resilience to potential infringements. Section 43 of the Education (No. 2) Act 1986 for England and Wales places a duty on every individual and body of persons concerned in the government of a provider to take such steps as are reasonably practicable to ensure that freedom of speech within the law is secured for members, students, employees and visiting speakers. It also requires providers to issue and keep up to date a code of conduct regarding freedom of speech. Every individual and body of persons concerned in the governance of the institution must take such steps as are reasonably practicable (including, where appropriate, the initiation of disciplinary measures) to secure that the requirements of the code of conduct are complied with.

Academic freedom and freedom of speech and expression have long been core tenets of academic culture in the UK. These concepts are nuanced and complex, and universities have a role to play in ensuring that these concepts are better understood by all members of the university community, including visiting staff and students. Universities should build understanding and consensus around these concepts by developing codes of conduct and policies that clearly set out the institution's position on them, as well as clearly demarcating the legal protections or legislation relevant to these concepts.

Universities need to set out clear statements on interference and to develop policies and procedures to ensure that these are upheld.

Key actions

- Develop and promote clear codes of conduct, policies and legal agreements that enshrine the avoidance of interference alongside the core values of academic freedom and freedom of speech.
- Promote open and transparent communication, debate, research and enquiry about what interference in academic freedom, freedom of speech and institutional autonomy might look like, and support staff and students to take responsibility for protecting against these infringements throughout their engagements and activities.
- Develop processes and mechanisms through which staff and students can report, raise concerns and receive support in relation to issues connected to academic freedom and freedom of speech, including issues arising from interference.
- Promote open and transparent communication, debate, research and enquiry about our shared values, and support staff and students to take responsibility for protecting against attempts to undermine them.

Encourage open and transparent discussion

To encourage open and transparent discussion about the importance of academic freedom and freedom of speech to the integrity and identity of UK higher education institutions, senior staff should promote debate, research and enquiry about these issues across their institutions. They should also raise awareness about the range of ways in which academic freedom and freedom of speech can be undermined by foreign interference. Universities will wish to engage a broad range of staff and students, including trade unions and student unions, professional services staff as well as academics, honorary staff, contractors and visitors to campuses through, for example, mandatory staff training.

Develop processes and mechanisms for raising concerns

Institutions should develop confidential mechanisms and spaces to allow both staff and students to raise any concerns that they may have relating to interference in the same way as they can for academic freedom and freedom of speech. This could involve adapting institutional ethics processes.

There should be clear and transparent lines of reporting in place to ensure that these cases are brought to the attention of senior leaders in a timely fashion and escalated where necessary.

As UK universities increase their operations overseas, they may find that the legal and social frameworks of other countries do not necessarily match those of the UK in respect of, for example, to anti-discrimination policies and the protection of individual rights. These should be assessed within the normal risk management framework.

While recognising that UK norms of academic freedom and freedom of speech may not be legally upheld in other countries, universities can still take measures to ensure that core values such as equality and diversity are respected within the university's own scope and working environment. For example, a university might publish a charter of values for staff working internationally, clearly stating the implications of the university's commitment to values of equality, diversity and respect, while recognising the laws and cultural norms of the country. These issues are explored further in Section 4.

Consider issues of extraterritorial jurisdiction

Individuals in the UK may be subject to laws passed by other countries that have extraterritorial application. These laws are not enforceable in the UK, but may pose challenges to future international travel, activities in or, in the case of international students or academics, return to certain countries. Extraterritorial jurisdiction could have a potentially chilling effect on activities in the UK, where academics and students may feel less able to participate in academic debate or progress research on certain topics that may be deemed sensitive by, and potentially subject to legal restrictions in, another nation state.

Institutions should consider the implications of laws with extraterritorial application for their students, staff and visitors. In response legislation with extraterritorial implications, some academic institutions have introduced protections for students. This has included, for example, identifying without modifying course material to students that might be considered politically sensitive in certain states. Institutions could also take steps to protect students by introducing the Chatham House rule to seminars or other oral discussions, and otherwise introducing measures that allow students to submit coursework anonymously.

There are specific challenges to consider in the delivery of online programmes that could potentially be recorded. Institutions will want to consider carefully how they can protect staff and students in these contexts.

Additional resources on promoting values

- EHRC
  Freedom of Expression: a guide for higher education providers and students' unions in England and Wales available at:
  https://www.equalityhumanrights.com/sites/default/files/freedom-of-expression-guide-for-higher-education-providers-and-students-unions-england-and-wales.pdf
- Kinzelbach, Saliba, Spannagel & Quinn Free Universities:
  Putting the Academic Freedom Index Into Action available at:
  www.gppi.net/media/KinzelbachEtAl_2020_Free_Universities.pdf
- Scholars at Risk
  Values at Home and in Partnership available at:
  www.scholarsatrisk.org/wp-content/uploads/2020/05/Values-at-Home-and-in-Partnerships.pdf
- University of Chicago
  Foundational Principles available at:
  https://freeexpression.uchicago.edu/foundational-principles/
- *Academic Freedom and Internationalisation Working Group Model Code of Conduct* available at:
  https://hrc.sas.ac.uk/networks/academic-freedom-and-internationalisation-working-group/model-code-conduct

2
PROTECTING YOUR PEOPLE

OVERVIEW

This chapter is intended to support your institution to protect its people, both students and staff, and visitors to your institution. The best way to achieve this is to develop and support a culture in which everyone is aware of security-related risks and understands their own exposure to them. UK universities are complex and diverse, and count citizens from across the world in their communities. Consequently, developing such a culture will not always be straightforward.

Every member of your community has a role to play in identifying, reporting and managing security-related risks. The first part of this chapter considers how these responsibilities might be made clear using internal and external communications. Your institution also has a role to play in communicating with government.

The second section of this chapter is concerned with protecting staff and students who are travelling and working overseas, and the steps that your institution might take to support those individuals.

Internal communications should be used to promote a culture of awareness and reinforce individual responsibilities to identify, report and manage security-related risks. External communications should promote transparency and build confidence in your institution's ability to undertake mutually beneficial international collaborations or partnerships. Institutions should share information with each other and government to identify best practice and increase resilience.

Senior leaders should have confidence that there are processes and procedures to ensure short- and long-term overseas activities to address security-related risks and to promote the safety and welfare of staff and students.

2.1: Internal and external communications and knowledge-sharing

Internal communications should be used to promote a culture of awareness and to reinforce individual responsibilities to identify, report and manage security-related risks. External communications should promote transparency and build confidence in your institution's ability to undertake mutually beneficial international collaborations or partnerships. Institutions should share information with each other and government to identify best practice and increase resilience.

This section outlines how existing communication channels should be used to promote mutually beneficial international collaborations or partnerships. It describes how institutions should engage with each other and government to strengthen sector responses to security challenges. This section is divided into three parts: internal communications, external communications and knowledge-sharing.

Internal communications

A positive, risk-informed culture develops out of a communal awareness and appreciation of risk. Internal communications are crucial when building a shared understanding of risk and should be available in a range of formats to cater to a diverse student and staff population. Communications should emphasise that everyone, including visiting students and staff, has a role to play in maintaining a secure campus environment and protecting their colleagues and peers. Communications should also detail the consequences of inadequate risk management.

Resources should be available to assist students and staff in understanding the risks associated with international collaborations and partnerships and how best to manage their specific obligations.[7] Supplementary training and institution-specific resources may also need to be developed by your institution. Training and resources should reflect the likely risks faced by individual members of your community.

External communications

External communications can be used to demonstrate that your institution is robust in its response to managing and mitigating security-related risks. We suggest that institutions publicly commit to the recommendations of this guidance and make as many of the policies and processes open as is practicable.

Knowledge-sharing

Sharing information and experiences across the sector and with government will assist the development of a common understanding of the nature and scale of the problem and best practice. To help coordinate activity and support institutions, identify a central point of contact for the issues set out in these guidelines and identify this individual to UUK. This will simplify cross-sector and sector–government engagement.

Your institution and staff will already be engaged with sector bodies and professional membership associations. These organisations will play an important role in sharing best practice and ideas to help your institution introduce the changes this document envisages. Over the next 12 months, UUK will systematically engage with sector bodies and professional membership associations to ensure that they have the information, advice and guidance they need.

It is important to engage in cross-sector dialogue (including those led by sector bodies) and to highlight your experiences, share best practice and build resilience to shared issues. Where appropriate, you should also engage with government. An understanding of the nature, frequency and scope of risk will support government in responding effectively through diplomatic or other channels.

Case study: Internal communications

The case studies in these guidelines are hypothetical, and they are intended to support the user to apply these guidelines in practice.

Scenario 1

A staff member has concerns about an existing research partnership. They believe that the partner is being used as a front to gain access to sensitive research undertaken at the institution. Representatives from the partner organisation have repeatedly demanded access to material beyond the scope of the contractual agreement. The staff member has denied all the partner's requests, but has become aware that the partner has submitted the same requests to other members of university staff.

[7] Such resources might include, for example, information about the risks of IP theft and academic freedom.

How would the staff member raise their concerns at your institution? Universities will need to consider:

- how reporting works within their current structures
- which person or group has ultimate oversight of reporting
- what safeguards are in place to prevent improper access.

In this scenario, the staff member recognised behaviours of concern. A further attempt to gain access to material was also rebuffed. What processes and procedures does your institution have in place to educate staff about potential risks, and ensure consistency of response?

Scenario 2

A postgraduate student received an unsolicited email from a researcher based outside the UK. The email congratulated the student on a recent co-authored journal article and asked if he would be willing to discuss the research and paper in more detail. The student did not recognise the emailer's name or home university, but, excited by the opportunity, responded saying he would be more than happy to discuss his work.

The student's supervisor was glad to see the paper had received attention and indicated she would join the call if possible. She suggested that the student fill in a short online form, as required by the department before any form of international engagement. The student submitted the form and was advised the next day that he should decline the meeting. The email he had received was sent to several researchers across the institution – on a wide variety of research topics – and was deemed to be suspicious and unlikely to be genuine.

In this scenario, the student followed departmental protocol and the request for a discussion about the research was ultimately declined. What internal processes do you have in place to support academics in making decisions in these and similar circumstances? You'll need to consider:

- whether internal processes are fit for purpose, and likely to be followed by staff
- how the institution can support academics to make decisions, and secure their buy-in for internal processes.

Additional resources on communications and knowledge-sharing

- CPNI
  Developing a Security Culture available at:
  https://www.cpni.gov.uk/developing-security-culture

- CPNI
  Optimising People in Security available at:
  https://www.cpni.gov.uk/optimising-people-security

2.2: Protecting staff and students travelling and working overseas

Senior leaders should have confidence that there are processes and procedures to address security-related risks, and to promote the safety and welfare of staff and students travelling overseas.

Students and staff travel all over the world in the course of their work and study. As a consequence of this travel, individuals may be exposed to specific, and in some cases severe, personal risks. This section considers how best to protect students, staff and institutional interests overseas.

It is important that you have robust processes and systems in place to assess the value and risk of all overseas engagements and activities – regardless of length or scale.

Plan travel arrangements

Many university staff and students regularly travel overseas in the course of their employment or study. In most cases, this short-term travel, irrespective of the purpose, will involve a similar degree of risk exposure as similar activity in the UK. However, in certain cases, individuals or universities may be exposed to significantly higher and unfamiliar risks. For example, students and academics involved in advanced or emerging technologies are likely to be of greater interest to local and national authorities.

Conduct due diligence and risk assessments

Section 1.2 above provides advice on implementing effective risk frameworks and due diligence processes for international partnerships. Specific processes are required for overseas travel that account for different risk environments, differences in legal, social and cultural norms in overseas countries, and changing operating environments abroad.

Where academics are area specialists, they should be engaged as experts on the country to inform university decision-making on risk levels and in providing information to staff.

Coherent safe travel policies must outline the steps needed for safely managing overseas travel and related activities, and outline clear approval processes, including processes for escalating high or unusual risks for institutional approval. Travel policies should also consider how export controls and other UK laws apply in each circumstance, and the implications of local and extraterritorial legislation on the person travelling overseas.

It is crucial that the processes in place are proportionate and applied to all international travel. Institutions should maintain records of overseas travel and draw on internal and external knowledge of the specific risks associated with travel to certain countries or regions. In addition, institutions should establish a formal method for monitoring and reviewing processes and procedures regularly, not just following an incident. See ‘Additional resources’ below for more sources of guidance.

Travel to certain countries requires special consideration and preparation. Processes should be in place to educate students and staff about specific security-related risks. This should include adequate training for students and staff to ensure that they understand the relevant policies and codes of conduct, as well as what is required of them and other obligations before travelling overseas.

Case study: Loss of data while overseas

The case studies in these guidelines are hypothetical, and they are intended to support the user to apply these guidelines in practice.

An overseas university extended a VIP invitation to a UK-based professor to present the keynote lecture at a national conference in their country. This presented a welcome opportunity for the professor to showcase her research, make senior-level contacts and to profile the department at a prestigious international conference. All the costs of attending would be covered for the professor and one guest, including business-class air travel, luxury hotel accommodation and subsistence costs. These were declared to the university ahead of travel.

As the professor had travelled to the country before and felt the risks to be negligible, a travel risk assessment was not completed. The professor signed a participation agreement with the host institution upon arrival.

The scenario

To present at the conference, the professor took her university laptop which, due to her institution's single-device policy, was her main device. She regularly charged the device in her hotel room and permitted conference organisers to plug in portable storage and other devices to facilitate her presentation. Her keynote lecture and visit were successful and well received.

Many months later, the professor was very concerned to see her unpublished research presented by a university based in the country where she had given the keynote speech. After reviewing the participation agreement for the conference, the professor realised she had signed over rights to the material presented at the conference, including the unpublished materials previewed during her presentation.

Lessons learned

- The institution had lacked appropriate risk assessment and governance processes to identify and allocate responsibilities for staff, students and academics ahead of all overseas travel.
- Appropriate travel approval and risk assessments are necessary ahead of all overseas travel.
- Complacency may influence the robustness of protocols followed in cases where a country or partner is already known to the institutions or the person travelling overseas.
- Travelling academics and researchers require training on relevant security policies, including the ways in which data may be stolen or compromised.

Additional resources on protecting staff and students

- CPNI
  Think securely about your business: Supporting business leaders to operate securely with overseas parties available at:
  www.cpni.gov.uk/secure-business
- CPNI
  Trusted Research: Countries and Conferences available at:
  www.cpni.gov.uk/system/files/Countries%20and%20Conferences%20Guide.pdf
- Foreign, Commonwealth & Development Office (FCDO)
  www.gov.uk/government/organisations/foreign-commonwealth-development-office

3
PROTECTING YOUR CAMPUSES

OVERVIEW

This chapter is intended to support your institution in protecting your campuses and the assets from security-related risks associated with potentially hostile activity. It focuses on cybersecurity, estates and visitors in the context of your institution's international partnerships and collaborations. It is not intended to provide general advice on campus security or physical and personnel security in the context of a wider range of threats, such as terrorist threats, and you should seek other resources for guidance on such matters.

Senior leaders must work together to protect UK campuses against security-related risks through a whole-organisation approach that ensures staff, students and visitors are aware of their responsibilities to protect digital and physical infrastructure and assets, including research, property and data.

This chapter includes a list of resources available from CPNI and NCSC and others.

3.1: Cybersecurity, estates and visitors

The UK's higher education institutions are proudly dynamic, diverse and international, bringing together staff, students and visitors from across the globe throughout the year. Open access to campuses and their associated sites is an important aspect of academic life that is necessarily built on a foundation of secure cyber networks, physical assets and campus buildings.

The threat to universities ranges from premeditated, sophisticated attacks on digital networks to more opportunistic breaches that exploit complacency and low cybersecurity awareness among individuals. The consequences of such breaches are not limited to your institution and may threaten the security and prosperity of the UK.

Develop and implement cybersecurity strategies

Senior leaders should ensure that cybersecurity strategies are developed and implemented. In parallel, institutions should develop effective oversight and reporting protocols for cybersecurity risks, including threat modelling and intelligence-sharing with government and the sector via mechanisms such as the Cyber Security Information Sharing Partnership (CiSP; see 'Additional resources' below).

Your institution will have a range of cybersecurity policies and procedures to manage access to software and hardware. However, as partnerships and collaborations come under greater scrutiny, it is likely that the frequency and sophistication of cyber-attacks will increase. You should ensure that your institution:

- uses published threat assessments to anticipate likely cyber-threats, such as the weekly threat assessments published by the NCSC
- understands and implements NCSC's 10 steps to cybersecurity
- considers certification through the NCSC Cyber Essentials scheme.

You should pay particular attention to protecting information of specific value, which is likely to be subject to greater risk. This might include, for example, research with potential economic value, politically and commercially sensitive material, sensitive enterprise data or data on your staff and students.

You should regularly review your cybersecurity risk response processes and, if possible, share your findings with other institutions and the government where this would support the sector to better respond to future incidents. In addition to developing an evidence-base, this exchange of information will increase the collective capacity of institutions, the sector and government to respond.

Appropriate training is particularly important for researchers working on high-security issues, controlled technologies or other areas of research that are subject to export control legislation. Institutions should develop policies and training packages that highlight the need to segregate research materials and limit and monitor access to sensitive data and information. Such policies include:

- segregation of sensitive research – separate out different areas of research so that data and information is not all held in one place, both physically and online
- access control – only users and partners with a valid requirement have access to this data and networks, with two-step identity verification where possible
- security of IT platforms – institutions should develop policies to ensure that staff and students understand the security of any collaborative IT platforms, especially those used by third parties
- protection from extraterritorial jurisdiction issues – consider carefully the risks faced by academics and students participating in online discussions about issues that some nation states might regard as sensitive and take steps to inform these individuals.

To support decision-makers, Jisc and UUK will issue an update of the 2013 guidance Cyber security and universities: managing the risk. This section will be updated with once the updated guidance is available.

Develop integrated estates and visitor policies

You should embed awareness of security-related issues into your existing estates and visitor policies. There needs to be robust policies and procedures for visitors to your institution, covering both staff and students.

As the case studies on loss of data (see Section 2.2) demonstrate, both digital and physical infrastructure are vulnerable to security infringements. All institutional policies and frameworks to protect campus infrastructure should cover particular physical security risks.

In relation to campus visitors, these policies might include:

- frameworks, policies and risk assessments that clearly distinguish between different types of visitor (for example, between professional and academic staff, undergraduate and postgraduate students, and short- and long-stay visitors)
- adequate checks on visitors before, on arrival and during their stay to restricted areas of the campus, including identity checks and checks on compliance with visa requirements, and checks to ensure their access is limited to the approved duration of their visit
- senior oversight and accountability for any visitor and visa agreements
- restrictions on access for visitors to courses or projects not cleared via their visa or ATAS application and clear processes for oversight and accountability for changing these during their visit
- clear advice, information and guidance for visitors and staff to inform them of the need to adhere to appropriate protocols during their time on campus.

Institutions will need to exercise their judgement as to how policies are designed and implemented. It is likely that the level of access to your campus will vary, depending on the type of activity being undertaken.

Annex 2 to these guidelines contains a series of guiding questions that might support institutions to develop strategies in response to the issues set out in this section.

Case study: Staff visitors

The case studies in these guidelines are hypothetical, and they are intended to support the user to apply these guidelines in practice.

Scenario

An international graduate research student based in the UK maintained connections with a research group at a university in their home country. The student sought permission to deliver a more formal partnership between the two research labs and offered to facilitate this. At the time, the research was not subject to export controls and, due to its initial small scale, the new partnership was exempt from sophisticated internal due diligence and oversight.

Following the establishment of the partnership, the student invited colleagues from the international lab to visit the UK institution, and made travel and other arrangements, and assisted with interpretation during their stay.

About a year into the partnership, a UK research supervisor became concerned that the relationship was very one-sided. Despite the overseas lab being extremely well-funded, it was slow to follow up on emerging research and technology.

Following a reassessment of the relationship, the supervisor realised that the research would likely become subject to export control restrictions and so terminated the partnership.

UK university staff later discovered that, during their visit, the delegation had taken detailed photographs of lab equipment for the purposes of reproducing the lab at their home institution. Inadequate supervision meant this breach was not identified at the time and the relationship was allowed to continue.

Lessons learned

- Overseas partners may attempt to access the early-stage development of technology and research before it is subject to export control legislation.
- Robust due diligence is necessary for all international partnerships, and may involve further investigation of the proposed partner and their identifiable associations to establish the size and scale of their operations.
- There is a need for strict protocols for all visiting staff and students, conducted prior to campus visits and tours.
- Visa invitation letters should only be authorised by suitably senior members of staff, not students.

As an exporter, you need to comply with strategic export controls and ensure that without an appropriate export licence is in place, where this is necessary. It is also possible that a compliance inspector from the Export Control Joint Unit (ECJU) will identify an irregularity during a compliance audit.

If this happens, it is very important to report the irregularity (sometimes known as 'voluntary disclosure') to HM Revenue & Customs (HMRC) as soon as possible, as they are responsible for the enforcement of strategic export controls. If the irregularity was found on an ECJU-compliance audit, the compliance inspector will have informed HMRC and you are strongly advised to do the same.

This information, as well as contact details for HMRC and the ECJU Joint Unit, can be found on www.gov.uk

Case study: Student visitors

The case studies in these guidelines are hypothetical, and they are intended to support the user to apply these guidelines in practice.

Scenario

Following an agreement between their two institutions, a cohort of overseas Master's students spent six months at a UK university. The students were expected to attend classes on campus and were assigned academic supervisors.

Although financial checks were completed before the agreement was finalised, further due diligence was not. Specific checks were not conducted to ensure compliance with UK strategic export controls. Supervisors had minimal interactions with the students, assuming the visit co-ordinator to be in regular contact with them. This left the students unsupervised and free to approach researchers and ask to collaborate with them, as is normal academic practice.

Following multiple approaches, several students became involved in highly sensitive, export-controlled research projects and gained access to restricted facilities. A request for access to a computing facility was granted by the co-ordinator with no additional oversight. The students shared the single-access card to visit the lab and other controlled areas.

Lessons learned

- The university should have conducted a review of the work being undertaken. If the technology was controlled, an export licence should have been requested.
- A range of techniques can be used to identify and exploit vulnerabilities at UK higher education institutions.
- Locations containing sensitive research and materials must be appropriately protected. Following this breach, the card-operated door was replaced with turnstiles, to prevent multiple entries with a single card.
- Clear management and oversight processes are required for visiting students and staff, including pre-arrival checks and regular points of contact. Supervisors of visiting staff must be aware of their obligations and responsibilities for the entirety of the visit.
- Staff working on export control or dual-use technologies must understand and fulfil their obligations to protect their research and university IP, both at home and abroad.

Additional resources on cybersecurity

- CPNI
  Think before you Link available at:
  www.cpni.gov.uk/security-campaigns/think-you-link
- CPNI
  Trusted Research: Guidance for Academia available at:
  www.cpni.gov.uk/trusted-research-guidance-academia
- Cyber Security Information Sharing Partnership (CiSP)
  www.ncsc.gov.uk/section/keep-up-to-date/cisp
- NCSC
  Cyber Essentials Certification Scheme available at:
  www.ncsc.gov.uk/cyberessentials/overview
- NCSC
  Risk management guidance available at:
  www.ncsc.gov.uk/collection/risk-management-collection
- NCSC Weekly threat reports
  www.ncsc.gov.uk/section/keep-up-to-date/threat-reports?q=&defaultTypes=report&sort=date%2Bdesc&start=0&rows=20
- NCSC
  Zero trust architecture design principles available at:
  www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles
- South, M (2018)
  Scaling a governance, risk, and compliance program for the cloud, emerging technologies, and innovation Amazon Web Services (AWS) available at:
  https://aws.amazon.com/blogs/security/scaling-a-governance-risk-and-compliance-program-for-the-cloud/
- *UCISA Information Security Management Toolkit* available at:
  www.ucisa.ac.uk/ismt

4
PROTECTING YOUR PARTNERSHIPS

OVERVIEW

This chapter is intended to support your institution to protect international partnerships. It is divided into two sections. The first considers the steps that universities need to undertake to safeguard research partnerships, with reference to the relevant legislation. The second considers how universities might safeguard transnational education partnerships.

The case studies exemplify the type of expected challenges and the practical actions that will protect intellectual property (IP), research integrity and compliance with relevant legislation, at all stages of the research cycle.

Senior leaders should take measures to ensure that research staff and students understand and adhere to processes that safeguard IP during international partnerships, comply with export control legislation and promote the ethics and integrity of research and data management.

4.1: Research security, intellectual property and export control compliance

The UK's world-leading research is increasingly open and collaborative. This presents significant and exciting opportunities, but also challenges. UK higher education institutions are subject to regular and targeted attempts by individuals and organisations from overseas seeking to improperly gain access to research and IP.

To assist institutions in making informed decisions about international partnerships and to protect their researchers and academic values, NCSC and CPNI developed Trusted Research.[8] This offers guidance of particular relevance to research in STEM subjects, dual-use technologies, emerging technologies and commercially sensitive research areas.

NCSC has also produced Trusted Research: Guidance for Senior Leaders, which outlines the essential considerations for you. You are strongly advised to familiarise yourself with these materials (see 'Additional resources' below for details.)

Key security threats and challenges that the research community should seek to manage and mitigate include:

- inadequate due diligence on international research partnerships, including those not part of formal, funded research projects
- inadequate oversight and monitoring of research partnerships and processes
- failure to adequately protect IP at the contractual stage and throughout the research partnership through IP 'leakage'
- IP theft by hostile actors, including through cyber-attacks and in-person theft of property
- non-compliance with export controls and dual-use technology legal frameworks.

[8] www.cpni.gov.uk/trusted-research

Conduct due diligence on all international research partnerships

Section 1.2 above sets out the overarching principles for due diligence on overseas partnerships. With respect to research collaboration, institutions must conduct due diligence proportionate to risk on all prospective overseas partners, for all types of engagement – formal partnerships and informal collaborations, funded and non-funded. In sensitive areas of research, including those covered by export controls, this will necessarily include any correspondence and/or discussion about the research, even if this is ad hoc or informal. In some cases, these processes will be audited by funding organisations, such as United Kingdom Research and Innovation (UKRI).

Implement policies and contractual agreements to protect intellectual property

The theft or misappropriation of research and IP can occur at any stage of the research cycle. Tools and frameworks exist to protect against this, including the Trusted Research guidance referred to previously (see 'Additional resources' below). The guidance is designed to give researchers, UK universities and industry partners confidence in international engagement, and to protect research and staff from potential theft, misuse or exploitation.

Your institution must have external work and conflict of interest policies to ensure that all staff, including honorary staff and both UK and non-UK nationals, declare any conflicts of interest or other professional obligations, relevant affiliations or legal contracts that are not part of their direct employment with the institution.

Ensure compliance with export control legislation

Researchers and research staff must be aware of the legal and regulatory frameworks relating to controlled technologies. Two prominent examples are export controls and the Academic Technology Approval Scheme (ATAS).

UK strategic export controls are intended to restrict the export and transfer of sensitive technology, information or strategic goods, with the aim of preventing the proliferation of weapons of mass destruction (WMDs), the illicit transfer of military technology and international threats such as terrorism (DfIT & ECJU, 2013). It is your responsibility to understand how export controls may apply to research or other activity conducted at your institution. Failure to comply with export control legislation is a criminal offence and may result in serious legal consequences.

The key point is that the terms 'technology' and 'information' have much broader definitions in legislation than might ordinarily or commonly be understood (see also Glossary).

To maximise compliance with export control legislation, individuals should:

- consider potential end-use possibilities of technology: it is the duty of researchers and their institutions to monitor potential end-uses of research, throughout the research life cycle. In some cases, research will have enduse applications that are unidentifiable in the early stages of development and continued monitoring is required
- inform researchers about the implications of intangible technology transfer: researchers must be aware that controlled sensitive information transmitted electronically (eg via social media, fax and email, videoconferencing, sharing screens remotely) and verbally (eg in telephone and face-to-face discussions) may still be subject to export controls. Further details can be found in DfIT & ECJU (2013).

ATAS requires all international students who are subject to UK immigration control and intend to study at postgraduate level in certain sensitive subjects to apply for an ATAS certificate. Applications must be made before an individual starts study in the UK or before being given access to university systems. Sensitive subjects include those that could be used in programmes to develop WMDs or their means of delivery. ATAS is operated by the Foreign, Commonwealth & Development Office (FCDO) and applies to all students whose nationality is outside the European Economic Area (EEA) and Switzerland, irrespective of the country of residence at the point of application. Further information on the ATAS scheme can be found on the FCDO website (see 'Additional resources' below).

Annex 3 of these guidelines contains checklists that will support your institution to manage challenges related to research security.

Case study: Overseas government contracts and appointments

The case studies in these guidelines are hypothetical, and they are intended to support the user to apply these guidelines in practice.

Following a recruitment process, an international professor was appointed to a UK university. Unknown and undisclosed to the university, the professor maintained paid involvement in a number of overseas government projects, including leading a national laboratory for applied military research. To progress this work without regular travel, the professor hosted fully funded visiting research students from his overseas laboratory to research in the UK. These students were used to transfer dual-use research and technologies to the overseas lab.

The scenario

Colleagues became concerned at the professor's workload and ill-health. Following an approach from university staff, the professor confessed to holding an external position and operating a shadow laboratory. The professor explained that the overseas contract placed him in a legally and ethically compromising position, prevented disclosure of the relationship without consent from the overseas government employer, and required him to work for many additional months a year. In addition, he had been instructed to curtail his UK employment in the next year and return to the home country and laboratory, in line with the existing contractual agreement. The majority of the funded visiting graduate research students, it transpired, were directly linked to the overseas country's military development activities.

Lessons learned

- Academic staff and students are sometimes recruited to circumvent export control regulations and transfer technology without authorisation.
- Although the institution had policies in place to identify overseas appointments and conflicts of interest, these procedures were not suitably robust. Institutions should promote a culture of vigilance, risk minimisation and support to identify vulnerabilities, particularly in relation to high-risk research areas.
- University policies must require all staff to disclose all overseas appointments, consultancies or honorary positions held. Universities must take a proactive approach to confirming guest academics' curricula vitae to ensure independent academic research is safeguarded.

Additional resources on research security, IP and export controls

Export control legislation

- DfIT & ECJU (forthcoming)
  Guidance for academics on export control legislation available at:
  These guidelines will be updated once the guidance is published.

- DfIT & ECJU (2020)
  Export controls: dual-use items, software and technology, goods for torture and radioactive sources available at:
  www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources

- DfIT & ECJU (2013)
  Do I need an export licence? available at:
  www.gov.uk/guidance/beginners-guide-to-export-controls
  (due to be updated December 2020)

- FCDO
  Academic Technology Approval Scheme (ATAS) available at:
  www.gov.uk/guidance/academic-technology-approval-scheme

Intellectual property

- Intellectual Property Office (2016)
  IP protection abroad: country guides available at:
  www.gov.uk/government/collections/ip-protection-abroad-country-guides

- Intellectual Property Office (2014)
  Intellectual asset management for universities available at:
  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/308072/ipasset-management.pdf

4.2: Transnational education partnerships

UK universities hold a reputation as world leaders in transnational education (TNE). UK institutions have nearly 700,000 students registered on UK programmes overseas, and the International Education Strategy (DfE & DfIT, 2019) sets an ambition to support the growth of this activity. Such activity brings significant opportunities for institutions, but also presents a wide range of risks that you should be aware of.

The risks associated with TNE go beyond financial and reputational concerns. When UK providers enter into TNE arrangements, they are subject to local regulations and must comply with instructions from local authorities. TNE operations may be at greater risk of security-related issues. A key issue for universities is to ensure that the core values of their institutions can be safeguarded in the context of local requirements. Universities may face a choice between complying with overseas government requirements or discontinuing activity.

Many universities have made significant progress in managing risks, having adopted integrated management models that enable them to assess, rank and mitigate risks across locations. However, these systems sometimes fail to integrate the risks affecting partner organisations overseas, in treating them as external. Sound risk-mitigation policies should acknowledge and assess the existence of risks that may affect overseas partners differently, and as far as possible, develop frameworks to co-own residual risk with transnational partners overseas.

Ensure thorough and regular due diligence on overseas partners

Different TNE activities carry different levels of risk. A branch campus with research-active staff can be more exposed to host government policy towards higher education than a partnership to validate a programme taught by a foreign provider. Senior leaders developing risk mitigation strategies within their due diligence process should:

- consider the level of exposure of their staff, students, research, IP and other resources to interference in the light of the specific TNE arrangements (e.g. subjects taught and related factors)
- draw on information from a diverse range of sources and use it to get a holistic understanding of the potential risks of operating overseas (e.g. through the FCDO, relevant UK embassy or consulate, the British Council, British Chamber of Commerce overseas and trusted partners)
- ensure that the TNE partner overseas has academic and institutional aims and objectives that are compatible with those of the UK institution
- understand the research partnerships and relationships of international institutions in their country of origin: for example, does the partner have links to governments and/or military research organisations?
- develop a framework and governance covering what research can be undertaken and what relationships they can engage in.

Include risks to institutional autonomy and academic freedom in risk registers and statements

Risks affecting institutional autonomy and different approaches to the relationship between the state and higher education providers have the potential to threaten the core values of UK higher education, particularly through infringement of academic freedom. Institutions should ensure that:

- risks related to institutional autonomy or academic freedom overseas are included in risk registers and risk statements, and are appropriately monitored, with oversight from the governing body
- the relationship of prospective and existing partners with government authorities in the overseas country is well understood, including the degree of autonomy, independence and transparency in the relationship.

Senior leaders with oversight of TNE activities have the responsibility to understand local values, laws, practices and expectations while developing policies and procedures to protect the values of UK higher education in an overseas context. These considerations should relate to institutional autonomy and to the relationship between the State and higher education providers. For example, in many places universities are public institutions with staff who are appointed by government and who are effectively civil servants. This should not in itself present a barrier to collaboration or partnership, but institutions have to consider whether this relationship presents a risk.

Senior leaders should remain open and transparent towards the tensions and conflicts associated with TNE operations based in foreign jurisdictions, while also seeking to manage trade-offs in a mutually respectful way.

Maintain a balance between robust centralised risk management and sufficient local autonomy

The majority of TNE ventures are built in partnership with overseas stakeholders. Often this is a requirement placed by local authorities and regulators, which occasionally become a formal partner in TNE operations. Institutions should ensure these partnerships maintain a balance between robust centralised risk management and sufficient local autonomy. Senior leaders should:

- consider how relevant policies and procedures compare with those used by partner institutions overseas, while embedding robust governance structures to raise and solve any issues that arise early on
- embed security-related risks in their risk management frameworks, including governance processes, risk policies, risk registers in the UK and overseas, assurance and audit processes, and business continuity planning in response to emergencies
- ensure that the interests of staff and students employed by or registered at the UK university and based overseas are appropriately safeguarded (eg for students registered at English providers through the University's Student Protection Plan)
- ensure that appropriate secure access processes and procedures, including to intangible assets, are in place, are appropriate to the sensitivity of the resources, and maintaining central oversight of who has access to those resources
- ensure that relevant and appropriate measures are taken to keep any cyber networks secure, as outlined in CPNI materials (see References for further information).

Jointly establish clear reporting lines and safe spaces for communication with local stakeholders

The most successful TNE partnerships combine mutual trust with robust oversight mechanisms. Not only are local partners best placed to identify and act on regulatory, economic or social changes affecting TNE, but often have the authority to perform certain legal acts that are essential for the educational operations of the UK university in the territories where it operates.

Gaining and retaining the trust of overseas stakeholders (students and their families, staff, partner providers, local authorities and regulators) is crucial for universities to be able to identify, manage and mitigate risk in TNE operations. Jointly established clear reporting lines and safe spaces for communication (including whistleblowing policies) applicable to overseas operations can favour early detection of security-related risks. However, note that joint risk assessments are rare, even though local partners are often more exposed. Senior leaders should:

- map out key actors with a stake in the education partnership, which may include local providers, authorities, businesses and employers, trade unions, non-governmental organisations, civil society organisations, UK embassies or consulates and professional bodies
- be aware of power dynamics and imbalances that may affect their relationship with local stakeholders, and between local stakeholders themselves
- where possible, assess vulnerabilities in the organisational and financial structure of the local partners, which may increase the risk of transmission of interference
- ensure support mechanisms are in place that help local stakeholders build and co-own risk management systems, especially those related to fraud, IP theft and corrupt practices
- establish appropriate communication channels (including whistleblowing policies) to allow local partners to raise concerns with the appropriate level of confidentiality and data and identity security.

Develop an exit strategy supported by comprehensive, rules-based arrangements and high-level principles

TNE partnerships evolve over time, and your institution should regularly review its scope. It is important to have an exit strategy in place if partnerships need to be ended. This strategy should be supported by high-level principles that have been communicated to all TNE partners, as well as comprehensive, rules-based arrangements that address issues such as academic freedom, IP and assets. Senior leaders should:

- clearly define a set of high-level principles that have been communicated to the TNE partner(s)
- follow rules-based arrangements that add protection to important issues such as academic freedom, IP, assets and staffing arrangements
- ensure students are protected in the event of partnership arrangements being terminated, through appropriate transition or other arrangements.

FORWARD LOOK

The UK has, and continues to benefit economically, socially and culturally from the internationalisation of the higher education sector. International collaborations and partnerships continue to drive the success of the sector. The higher education sector, working with the UK government, wishes to build on that success, cementing the role of UK universities as world leaders in education and research.

The UK government has published ambitious strategies for international education and international research, in the form of the International Education Strategy (DfE & DfIT, 2019) and the UK Research and Development Roadmap (HM Government, 2020). The strategy and the roadmap envisage an increase in activity, both in the volume and value of education exports, and an increase in international research collaborations and partnerships. As those strategies acknowledge, that expansion cannot come at any cost, and these guidelines are part of a wider effort intended to ensure that the growth of such activity does not compromise the values of UK universities or the national interest.

The recommendations and changes envisaged in these guidelines will support institutions to protect their reputation and values, their staff, estates and partnerships. This will require changes in culture as well as policies and processes to ensure that individuals are well supported to make the right decisions.

Working with others, including the UK government, UUK's efforts have been focused on securing changes in awareness and understanding within the higher education sector of security-related issues, including through the production of these guidelines. We remain committed to this work, and will undertake an evaluation of this guidance. We will publish an update on our progress in autumn 2021.

Sector bodies and professional membership bodies have a major role to play in driving this agenda forward. As part of the evaluation of this guidance, we will consider what other changes need to happen within the higher education sector to help individuals and universities manage security-related risks.

The UK government has a major role to play in supporting individuals and institutions in addressing the threats and mitigating the risks set out in these guidelines. We will continue to work with the government to ensure we have a clear, collaborative and constructive approach towards protecting and promoting growth in research and innovation activities, institutional autonomy, academic freedom and freedom of speech in the context of growing security challenges.

GLOSSARY

academic freedom: while difficult to define precisely, academic freedom is generally recognised as the freedom of academics in the UK higher education sector to: teach and discuss; carry out research, publish the results and make them known; freely express opinions around the academic institution or system in which they work; participate in professional or representative academic bodies; not be censored; and fulfil their functions without discrimination or fear of repression.

The above is underpinned by the provisions of: the 1997 UNESCO Recommendation concerning the Status of Higher-Education Teaching Personnel (Section VI(A)); the Education Reform Act 1998 Section 202(2)(a); and the Higher Education and Research Act 2017 Section 2(8)(c).[9]

branch campus: an entity that is owned, at least in part, by a foreign education provider, that is operated in the name of the foreign education provider, and that provides an entire academic programme, substantially on site, leading to a degree awarded by the foreign education provider.

influence: all governments, including the UK government, try to influence deliberations on issues of importance to them. These activities, when conducted in an open and transparent manner, are a normal aspect of international relations and diplomacy and can contribute positively to public debate.

intangible asset: something valuable that is not material. The context of a higher education institution, intangible assets could include inventions, works of authorship, software, data, know-how, experimental designs, and technical information.

interference: malign activity by another state or those acting on its behalf that is designed to have a detrimental effect on the interests of the UK. This activity can be deceptive, coercive or corruptive, and is not limited to the covert domain. It includes the use of agents of influence, leverage of investments, financial inducement, disinformation and other cyber-activities.

internationalisation: a broad term as applied to higher education, but used in these guidelines, to describe the purposeful integration of international and intercultural dimensions into aspects of university activity.[10]

research integrity: while there is no universal definition of research integrity, the concordat to support the integrity of research identifies five core elements (under commitment 1). The Singapore Statement on Research Integrity (2010), provides a further definition. In addition, the UK Research Integrity Office has set out principles of research integrity in its Code of Practice (UKRIO, 2009).

security-related: an umbrella term that describes a broad range of issues and risks that are associated with internationalisation. 'Security-related' risks referred to in these guidelines can be broadly grouped into two categories: attempts by overseas/hostile/external actors or those acting on their behalf to illegitimately acquire academic research and expertise; and/or interfere with academic discourse.

[9] https://hrc.sas.ac.uk/sites/default/files/files/AFIWG/AFIWG%20-%20DRAFT%20MODEL%20CODE%20OF%20CONDUCT%20final.pdf

[10] https://link.springer.com/chapter/10.1007/978-3-319-20877-0_5

technology: under export controls, used to cover information in the form of 'technical data' and 'technical assistance' (see the academic guidance published by the Export Control Joint Unit for full details).

transnational education (TNE): all types of higher education study programmes, or different sets of courses of study or educational services, in which learners are located in a country that differs from the one where the awarding institution is based, e.g. branch campuses, fly-in faculty, and online and/or distance learning.

ANNEX 1: SUMMARY OF RESOURCES AVAILABLE TO INSTITUTIONS

1: Protecting your reputation and values

1.1: Building resilience to security-related issues

- CPNI
  Trusted Research: Guidance for senior leaders available at:
  www.cpni.gov.uk/system/files/Trusted%20Research%20Guidance%20for%20Senior%20Leaders.pdf

1.2: Due diligence

- ARMA
  Consolidated Approach to Assurance and Due Diligence project available at:
  https://arma.ac.uk/first-output-from-the-consolidated-approach-to-assurance-and-due-diligence-project/

- CPNI
  Campaign implementation plan available at:
  www.cpni.gov.uk/system/files/Trusted%20Research%20Implementation%20Guide.pdf

- CPNI
  Checklist: Evaluating research proposals available at:
  www.cpni.gov.uk/system/files/Trusted%20Research%20Checklist%20for%20Academia.pdf

- CPNI
  Trusted Research: Guidance for Academia available at:
  www.cpni.gov.uk/trusted-research-guidance-academia

Sources to help identify international collaborations or partnerships that fall into the high-risk category:

- UN Sanctions List
- US export entity control list
- HM Treasury's financial sanctions targets
- Country corruption index
- Human Freedom Index
- World Justice Project Rule of Law Index

Templates and frameworks for due diligence

- Economist Intelligence Unit (EIU) (country overviews and risk briefings)
  https://country.eiu.com/All

- FCDO & DfIT
  Overseas business risks available at:
  www.gov.uk/government/collections/overseas-business-risk

- Global Edge (sources of statistical information for countries worldwide)
  https://globaledge.msu.edu/global-insights/by/country

1.3: Promoting the values of UK higher education

- EHRC
  Freedom of Expression: a guide for higher education providers and students' unions in England and Wales available at:
  www.equalityhumanrights.com/sites/default/files/freedom-of-expression-guide-for-higher-education-providers-and-students-unions-england-and-wales.pdf

- Kinzelbach, Saliba, Spannagel & Quinn
  Free Universities: Putting the Academic Freedom Index Into Action available at:
  www.gppi.net/media/KinzelbachEtAl_2020_Free_Universities.pdf

- Scholars at Risk
  Values at Home and in Partnership available at:
  www.scholarsatrisk.org/wp-content/uploads/2020/05/Values-at-Home-and-in-Partnerships.pdf

- University of Chicago
  Foundational Principles available at:
  https://freeexpression.uchicago.edu/foundational-principles/

2: Protecting your people

2.1: Internal and external communications and knowledge-sharing

- CPNI
  Developing a Security Culture available at:
  www.cpni.gov.uk/developing-security-culture

- CPNI
  Optimising People in Security available at:
  www.cpni.gov.uk/optimising-people-security

2.2: Protecting staff and students travelling and working overseas

- CPNI
  Think securely about your business: Supporting business leaders to operate securely with overseas parties available at:
  www.cpni.gov.uk/secure-business

- CPNI
  Trusted Research: Countries and Conferences available at:
  www.cpni.gov.uk/system/files/Countries%20and%20Conferences%20Guide.pdf

- Foreign, Commonwealth & Development Office (FCDO)
  www.gov.uk/government/organisations/foreign-commonwealth-office

3: Protecting your campuses

3.1: Cybersecurity, estates and visitors

- CPNI
  Think before you Link available at:
  www.cpni.gov.uk/security-campaigns/think-you-link
- CPNI
  Trusted Research: Guidance for Academia available at:
  www.cpni.gov.uk/trusted-research-guidance-academia
- Cyber Security Information Sharing Partnership (CiSP)
  www.ncsc.gov.uk/section/keep-up-to-date/cisp
- Gaehtgens, F, Data, A, Kelley, M (2009)
  Remove Standing Privileges Through a Just-in-Time PAM Approach Gartner Research available at:
  www.gartner.com/en/documents/3957029/remove-standing-privileges-through-a-just-in-time-pam-ap
- NCSC
  Cyber Essentials Certification Scheme available at:
  www.ncsc.gov.uk/cyberessentials/overview
- NCSC
  Risk management guidance available at:
  www.ncsc.gov.uk/collection/risk-management-collection
- NCSC
  Weekly threat reports
  www.ncsc.gov.uk/section/keep-up-to-date/threat-reports?q=&defaultTypes=report&sort=date%2Bdesc&start=0&rows=20
- NCSC
  Zero trust architecture design principles available at:
  www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles
- South, M (2018) Scaling a governance, risk, and compliance program for the cloud, emerging technologies, and innovation Amazon Web Services (AWS) available at:
  https://aws.amazon.com/blogs/security/scaling-a-governance-risk-and-compliance-program-for-the-cloud/

4: Protecting your partnerships

4.1: Research security, intellectual property and export control compliance

- DfIT & ECJU (2020)
  Export controls: dual-use items, software and technology, goods for torture and radioactive sources available at:
  www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources

- DfIT & ECJU (2013)
  Do I need an export licence? available at:
  www.gov.uk/guidance/beginners-guide-to-export-controls
  (due to be updated December 2020)

- FCDO Academic Technology Approval Scheme (ATAS) available at:
  www.gov.uk/guidance/academic-technology-approval-scheme

- Intellectual Property Office (2016)
  IP protection abroad: country guides available at:
  www.gov.uk/government/collections/ip-protection-abroad-country-guides

- Intellectual Property Office (2014)
  Intellectual asset management for universities available at:
  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/308072/ipasset-management.pdf

4.2: Transnational education partnerships

- DfE & DfIT (2019)
  International Education Strategy: global potential, global growth available at:
  www.gov.uk/government/publications/international-education-strategy-global-potential-global-growth/international-education-strategy-global-potential-global-growth

ANNEX 2:
GUIDING QUESTIONS FOR CYBERSECURITY, ESTATES AND VISITOR POLICIES

1. Are security-related risks and overseas threats sufficiently embedded in cybersecurity strategies, estates policies and visitor procedures and protocols?
2. Is there sufficient join-up between those responsible for the oversight and discharge of strategies relating to the protection of campuses and infrastructure, whether through the protection of digital systems, physical property or visitor procedures and protocols? What mechanisms are in place to support this join-up?
3. Are periodic risk assessments performed to evaluate risk in each building, taking into consideration multiple factors such as the type of research activities taking place, including non-disclosure agreements (NDAs), the range of visitors and shipping to and from the building?
4. Are the risk assessments undertaken by personnel with expertise and responsibilities in the various areas of interest, including the protection of digital systems, physical property and visitor procedures and protocols?
5. Are there effective procedures in place to review regularly access to sensitive data and facilities by those who have access?

ANNEX 3:
CHECKLISTS FOR RESEARCH SECURITY, INTELLECTUAL PROPERTY AND EXPORT CONTROLS

Research security checklists

Due diligence on international research partnerships

1. How clear are requirements to undertake proportionate risk assessments before international research collaborations start?
2. Who has responsibility for conducting risk assessments on overseas research projects?
3. What policies exist in the university to identify research contracts that require additional oversight due to the nature of the research and/or the type of partnership?
4. How does your institution investigate the size and type of research operations being undertaken by a potential new research partner?
5. What are your institutional processes for monitoring small or informal research partnerships that are established by individual academics or principal investigators?
6. What additional resources and support are available to provide ongoing due diligence on high-risk international research partnerships?
7. Have you taken steps to ensure that any translated versions of contractual agreements include identical terms and conditions?

Policies and contractual agreements to protect intellectual property

1. What policies, tools and frameworks does your institution use to protect intellectual property (IP)?
2. Who has responsibility for signing off and monitoring contractual agreements on research collaborations?
3. What is the process for contracts and agreements put in place for non-funded research projects, such as one-to-one research collaborations between academics in the UK and overseas?
4. What processes are in place to deal with breaches of, or changes to contractual research agreements?
5. Are researchers – both those based in the UK and those based overseas – asked to disclose external work obligations and conflicts of interest on a regular basis?
6. What kind of training is available to support researchers to take measures to protect against IP theft or leveraged transfer through cybersecurity infringements or the theft of personal property?

Dual-use technologies and export control legislation

1. Do researchers understand the term 'dual-use' and know how it affects them?
2. How do researchers reasonably consider the potential for their research to become dual-use?
3. In what ways might researchers consider the potential for their research to be used for purposes that are inconsistent with promoting economic, social and security benefits for the UK?
4. What strategies are in place to ensure compliance with export control legislation and other relevant legislative frameworks? What guidance exists on when researchers should seek further advice, internally or external to the university?
5. Is there a risk that investment might seek to or be able to undermine or circumnavigate UK strategic export controls or similar measures?

REFERENCES

- Beelen J., Jones E. (2015) Redefining Internationalization at Home. In: Curaj A., Matei L., Pricopie R., Salmi J., Scott P. (eds) The European Higher Education Area. Springer, Cham. https://link.springer.com/chapter/10.1007%2F978-3-319-20877-0_5
- Cabinet Office (2020) *Guidance for General Grants: Minimum Requirement Seven: Risk, Controls and Assurance* available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896343/Grants-Standard-SEVEN-Due-Diligence-and-Fraud-Risk.pdf
- CPNI *Campaign implementation plan* available at: www.cpni.gov.uk/system/files/Trusted%20Research%20Implementation%20Guide.pdf
- CPNI *Checklist: Evaluating research proposals* available at: www.cpni.gov.uk/system/files/Trusted%20Research%20Checklist%20for%20Academica.pdf
- CPNI *Developing a Security Culture* available at: www.cpni.gov.uk/developing-security-culture
- CPNI *Think before you Link* available at: www.cpni.gov.uk/security-campaigns/think-you-link
- CPNI *Think securely about your business: Supporting business leaders to operate securely with overseas parties* available at: www.cpni.gov.uk/secure-business
- CPNI *Trusted Research: Countries and Conferences* available at: www.cpni.gov.uk/system/files/Countries%20and%20Conferences%20Guide.pdf
- CPNI *Trusted Research: Guidance for Academia* available at: www.cpni.gov.uk/trusted-research-guidance-academia
- CPNI *Optimising People in Security* available at: www.cpni.gov.uk/optimising-people-security

- DfE (2019)
  UK revenue from education related exports and transnational education activity in 2017 available at:
  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/850263/SFR_Education_Exports_2017_FINAL.pdf

- DfE & DfIT (2019)
  International Education Strategy: global potential, global growth available at:
  www.gov.uk/government/publications/international-education-strategy-global-potential-global-growth/international-education-strategy-global-potential-global-growth

- DfIT & ECJU (2020)
  Export controls: dual-use items, software and technology, goods for torture and radioactive sources available at:
  www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources

- DfIT & ECJU (2013)
  Do I need an export licence? available at:
  www.gov.uk/guidance/beginners-guide-to-export-controls

- EHRC
  Freedom of Expression: a guide for higher education providers and students' unions in England and Wales available at:
  www.equalityhumanrights.com/sites/default/files/freedom-of-expression-guide-for-higher-education-providers-and-students-unions-england-and-wales.pdf

- Eversheds
  International Partnerships – Legal Guide for UK Universities available at:
  www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/International/LegalGuideFINALMarch13.pdf

- FCDO & DfIT *Overseas business risks* available at:
  www.gov.uk/government/collections/overseas-business-risk

- Gaehtgens, F, Data, A, Kelley, M (2009)
  Remove Standing Privileges Through a Just-in-Time PAM Approach
  Gartner Research available at:
  www.gartner.com/en/documents/3957029/remove-standing-privileges-through-a-just-in-time-pam-ap

- HM Government (2020)
  UK Research and Development Roadmap available at:
  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896799/UK_Research_and_Development_Roadmap.pdf

- *Human Rights Consortium (2020) Model Code of Conduct* available at:
  https://hrc.sas.ac.uk/networks/academic-freedom-and-internationalisation-working-group/model-code-conduct

- Kinzelbach, Saliba, Spannagel & Quinn
  Free Universities: Putting the Academic Freedom Index Into Action available at:
  www.gppi.net/media/KinzelbachEtAl_2020_Free_Universities.pdf
- Intellectual Property Office (2016)
  IP protection abroad: country guides available at:
  www.gov.uk/government/collections/ip-protection-abroad-country-guides
- Intellectual Property Office (2014)
  Intellectual asset management for universities available at:
  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896799/UK_Research_and_Development_Roadmap.pdf
- NCSC
  Cyber Essentials Certification Scheme available at:
  www.ncsc.gov.uk/cyberessentials/overview
- NCSC
  Risk management guidance available at:
  www.ncsc.gov.uk/collection/risk-management-collection
- NCSC
  Trusted Research: Guidance for senior leaders available at:
  www.cpni.gov.uk/system/files/Trusted%20Research%20Guidance%20for%20Senior%20Leaders.pdf
- NCSC
  Weekly threat reports –
  www.ncsc.gov.uk/section/keep-up-to-date/threat-reports?q=&defaultTypes=report&sort=date%2Bdesc&start=0&rows=20
- NCSC
  Zero trust architecture design principles available at:
  www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles
- Scholars at Risk
  Values at Home and in Partnership available at:
  www.scholarsatrisk.org/wp-content/uploads/2020/05/Values-at-Home-and-in-Partnerships.pdf
- South, M (2018)
  Scaling a governance, risk, and compliance program for the cloud, emerging technologies, and innovation Amazon Web Services (AWS) available at:
  https://aws.amazon.com/blogs/security/scaling-a-governance-risk-and-compliance-program-for-the-cloud/
- University of Chicago
  Foundational Principles available at:
  https://freeexpression.uchicago.edu/foundational-principles/

- UUK (2019)
  International facts and figures 2019 available at:
  www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/Intl-facts-figs-19.aspx

Websites

- ATAS (Academic Technology Approval Scheme) available at:
  www.gov.uk/guidance/academic-technology-approval-scheme
- Centre for the Protection of National Infrastructure (CPNI)
  www.cpni.gov.uk
- Cyber Security Information Sharing Partnership (CiSP)
  www.ncsc.gov.uk/section/keep-up-to-date/cisp
- Economist Intelligence Unit (EIU) (country overviews and risk briefings)
  https://country.eiu.com/All
- Foreign, Commonwealth and Development Office (FCDO)
  www.gov.uk/government/organisations/foreign-commonwealth-development-office
- Global Edge (sources of statistical information for countries worldwide)
  https://globaledge.msu.edu/global-insights/by/country
- National Cyber Security Centre (NCSC)
  www.ncsc.gov.uk
- Trusted Research
  www.cpni.gov.uk/trusted-research

Copyright

Universities UK is the collective voice of 139 universities in England, Scotland, Wales and Northern Ireland. Our mission is to create the conditions for UK universities to be the best in the world; maximising their positive impact locally, nationally and globally. Universities UK acts on behalf of universities, represented by their heads of institution.

Universities UK

Woburn House
20 Tavistock Square
London, WC1H 9HQ

T: +44 (0)20 7419 4111
E: info@universitiesuk.ac.uk
W: universitiesuk.ac.uk
@UniversitiesUK

October 2020
ISBN: 978-1-84036-455-2