
National Protective
Security Authority
TRUSTED
RESEARCH
COUNTRIES AND CONFERENCES
National Cyber
Security Centre
a part of GCHQ

FOREWORD

Trusted Research is a campaign by the UK's national technical authorities for security to raise awareness of the risks to research collaborations, which may involve working with an organisation or research partners with links to a nation whose democratic and ethical values are different from our own.

For many academics and researchers, attending conferences across the globe is integral to their role. Where a conference is being held can be an important factor in assessing the risks and threats that academics may face.

Countries and Conferences should be read alongside Trusted Research Guidance for Academia. It is aimed at academics who are involved in international research collaborations and provides advice and guidance on some of the main challenges presented when working or travelling overseas. It will be particularly relevant in the following situations:

- Meetings and conferences
- Fieldwork
- Hosted research
- Visiting researchers
- Conference speakers
- Teaching
- Visits to academic institutions
- Visits to overseas industrial partners or sponsors

Protect yourself

The UK has a long history of protecting academic freedom which is enshrined in law. This is not the case in some other countries, including those that you might visit. Academic institutions, individual departments and managers have a duty of care to their staff when overseas, and this should include security considerations.

Before undertaking a research or teaching trip overseas you should consider:

- Whether you understand the cultural and legal landscape within that country and what impact this will have on the way in which you conduct research or teaching. The protection of academic freedoms in the UK will not automatically apply when visiting other countries
- Who within your university or institution you need to notify or ask permission to travel
- Whether, if working with industry partners, there may be a contractual arrangement to notify them of travel and overseas working, particularly if it could constitute a conflict of interest

Understand the risk

Before you travel you should consider completing a risk assessment. Take a proportionate approach which considers the country you are visiting and the reason for your visit. Keep this under review up to the point of departure, as well as during the trip, as the situation may change quickly.

Your primary source of information for advice in relation to overseas travel should always be the Foreign and Commonwealth Office (FCO) website. The Intellectual Property Office (IPO) also provides specific advice and guidance on the intellectual property (IP) protections afforded in a range of different countries. You should also check the individual policies and procedures that your institution operates.

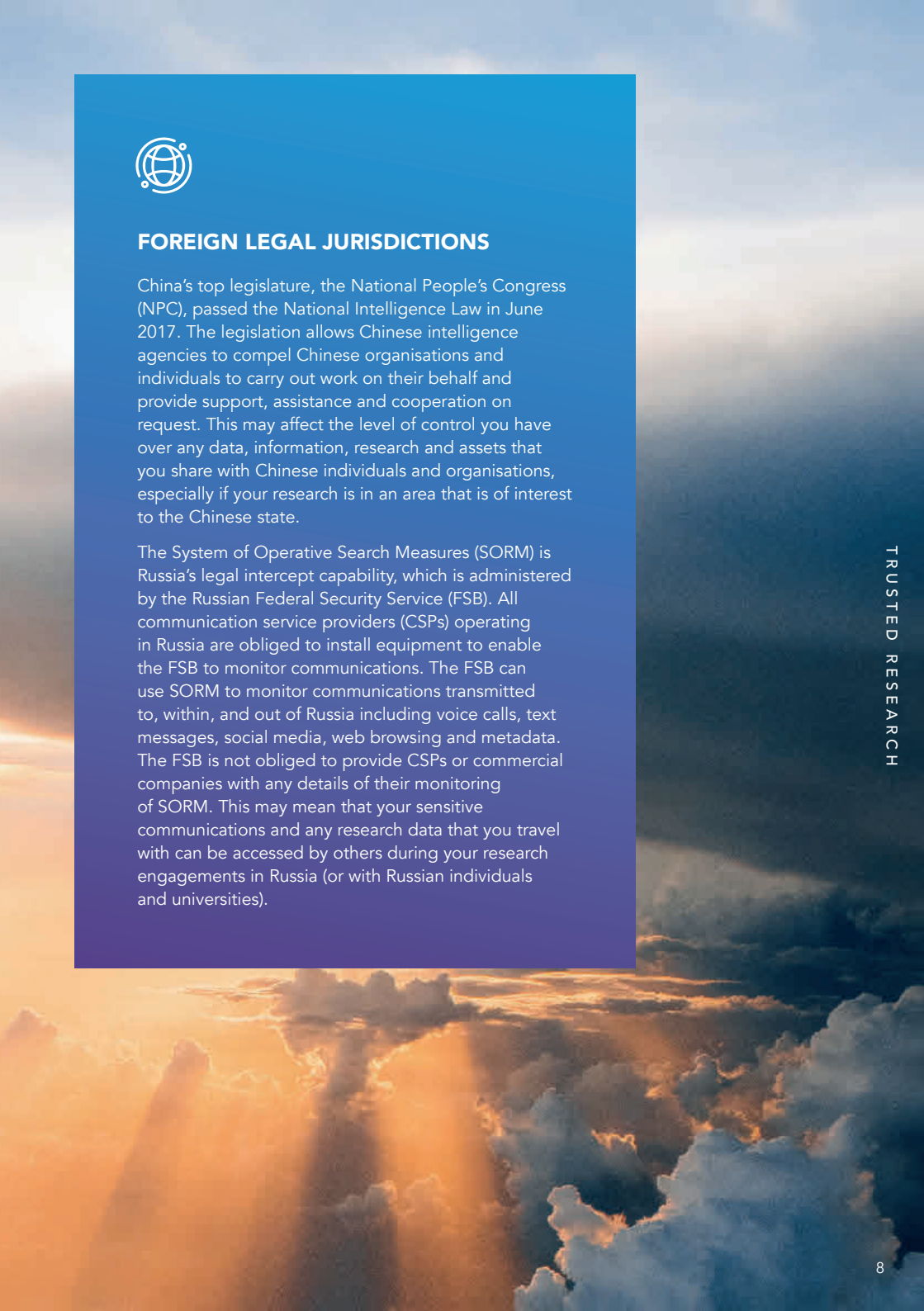
When assessing the risk, you may wish to consider the following questions about your destination country:

- What sort of protection is provided for academic freedom?
- What is the Foreign and Commonwealth Office advice?
- Are you travelling to a country where sanctions may have been imposed by the UK?
- Is the nature of the research that you undertake sensitive?
- What is the legal and legislative environment and is there potential for your activities to be misunderstood?
- Could your research or academic activities be perceived as a threat to a country whose democratic and ethical values differ from our own?

Compliance in foreign jurisdictions

If you are collaborating with an international partner there may be laws and regulations which you need to comply with in your collaborator's country. Most countries will maintain some form of export control, they may have laws which restrict their institution's ability to share data or research outcomes, and the legal protections around IP may also differ in those jurisdictions.

You should not assume that your research partner will take responsibility for such compliance, and you should be aware of any requirements that impact the collaboration.



FOREIGN LEGAL JURISDICTIONS

China's top legislature, the National People's Congress (NPC), passed the National Intelligence Law in June 2017. The legislation allows Chinese intelligence agencies to compel Chinese organisations and individuals to carry out work on their behalf and provide support, assistance and cooperation on request. This may affect the level of control you have over any data, information, research and assets that you share with Chinese individuals and organisations, especially if your research is in an area that is of interest to the Chinese state.

The System of Operative Search Measures (SORM) is Russia's legal intercept capability, which is administered by the Russian Federal Security Service (FSB). All communication service providers (CSPs) operating in Russia are obliged to install equipment to enable the FSB to monitor communications. The FSB can use SORM to monitor communications transmitted to, within, and out of Russia including voice calls, text messages, social media, web browsing and metadata. The FSB is not obliged to provide CSPs or commercial companies with any details of their monitoring of SORM. This may mean that your sensitive communications and any research data that you travel with can be accessed by others during your research engagements in Russia (or with Russian individuals and universities).

SUPPORTING STAFF OVERSEAS

If you have staff working in a country whose democratic and ethical values are different from our own, your risk assessment could include the following:

- If something happens to one of your colleagues when they are working overseas, who should they report it to?
- How often do you check whether they have concerns or issues?
- What agreements are there with the institution that will be hosting them overseas?
- What are the rules and laws that they are required to comply with in that country?
- Do any laws conflict with any of the agreements that you have made with that institution?
- Will the work that they conduct be subject to UK export control?
- Are your colleagues aware of the export control laws, national security laws and IP arrangements in the country where they are working?

Nationals of a country which may not have the same legal or constitutional rights as the UK may be more vulnerable when travelling. Managers should exercise a duty of care in such circumstances where there is a risk that they may face duress.

Staff negotiating overseas research collaborations also assume greater risk on behalf of their institutions. Refer to the Trusted Research Guidance for Academics to ensure that they have a good understanding of the risks and ensure that you have set a clear framework and scope for their engagement.

Before you travel

Make sure you establish the correct visa requirements for the country you are visiting. If working abroad or attending an academic conference, a tourist visa may not be appropriate and you may require a research or work visa. You should also establish whether there are any specific clearances required for the research that you intend to undertake.

Conferences provide a unique opportunity to share ideas and progress with colleagues in a similar field, but you should consider whether there are any restrictions to you presenting your research. Depending on the nature of your research you may be subject to contractual restrictions from funders or your academic institution. When presenting research in another country you should also consider whether it could be subject to export control and consult with Export Control Joint Unit (ECJU) if you are unsure.

Think carefully about whether you need to take all of your research with you and whether it is appropriate to present or discuss it on your trip. In some countries, authorities could easily and legally access a laptop, for example at customs, and copy all the contents.

Other issues to consider:

- Could your involvement put you in breach of your contractual undertakings or present a conflict of interest for you or the university?
- Do you require authorisations from your institution or department?
- Do you have a duty to inform or seek agreement from industry partners?
- If accepting payment or expenses from an organisation, do you need to declare them to your department, institution or HMRC?
- Before you travel, what information, electronic devices and media do you need to take?
- Do you have appropriate insurance in place for the travel and work that you are undertaking?

Cyber security advice

When travelling overseas, it is almost certain that you will want to take mobile IT devices with you, such as a laptop, tablet and/or mobile phone. However, think carefully about the work and personal information they contain and what the impact would be if any of the devices were lost or stolen. Your institution's IT department will be able to advise you how to manage your information, and may well be able to provide you with clean devices that contain only the information essential to your trip.

If you do decide to take devices, here are the basic cyber security tips that you should consider for your trip:

Before travelling

- Check with your network operator or IT department whether your technology will work abroad and what costs are involved. It may be safer and cheaper to buy a pay-as-you-go phone
- Make sure your devices are password/passcode protected and use other security features, such as fingerprint recognition. Passwords/passcodes should be unique for each account and device
- Many email and social media providers offer two-step verification. You should turn this on for important accounts; it makes it harder for other people to access your accounts and can provide alerts if others are attempting to access your accounts without your permission
- Consider removing data or information from devices that you would not want to share; this may include research or information about IP
- Consider the use of Virtual Private Networks (VPNs) to manage communication back to the UK. However, be aware of any local rules on VPN usage, which is normally permitted but access must be provided if requested by law enforcement
- Consider activating device-wide encryption – see page opposite for the benefits of encrypting the data we store
- Turn on the ability to wipe your phone should it become lost. Back up all your data and photos before you travel
- Make sure all your software and apps are up to date prior to leaving the UK. If you are taking a laptop, make sure your antivirus is turned on, USB autorun is turned off, the laptop is password protected and will not automatically connect to Wi-Fi networks
- Never download apps from unofficial providers, either in the UK or abroad. Unofficial app stores cannot be trusted; there is no way of knowing if the app is genuine

BENEFITS OF ENCRYPTION

Consult your university or institution IT department on what policies are in place for taking devices overseas and for connecting back to your institution.

Encrypting data while it is being stored (e.g. on a laptop, mobile, USB or back-up media, databases and file servers) provides effective protection against unauthorised or unlawful processing. It is especially effective to protect data against unauthorised access if the device storing the encrypted data is lost or stolen.

Depending on the circumstances, an effective and appropriate encryption solution can also be a means of demonstrating compliance with the security requirements of the GDPR. The Information Commissioner's Office (ICO) has considered encryption to be an 'appropriate technical measure'; in cases where data is lost or unlawfully accessed and encryption was not used, they may consider regulatory action.

The ICO recommends that "[p]ersonal data should be stored in an encrypted form to protect against unauthorised access or processing, especially if the loss of the personal data is reasonably likely to occur and would cause damage or distress to individuals."

While abroad

When overseas it is tempting to think that you may be 'out of sight and out of mind'. Yet engaging in inappropriate activities, even if they are not illegal in the UK or at the destination, can have a lasting impact. Use your judgement to determine whether an activity could leave you vulnerable to external pressure or cause reputational damage to you, your organisation and the UK.

Be aware of unusual requests or approaches, such as questioning about more sensitive areas of work or scenarios where you are pressured into sharing information and detail that you feel uncomfortable with. In all cases respond with a polite but firm refusal. Consider carefully what you do with gifts and whether you need to declare anything of financial value to your department, institution or HMRC. Think carefully and seek advice from your legal services team before signing any undertakings relating to conference attendance or presentation.

Trust your instinct. If something appears unusual or suspicious, report it to your head of department or appropriate university authorities on your return.

Observing the following advice can also ensure that you keep yourself and your information secure:

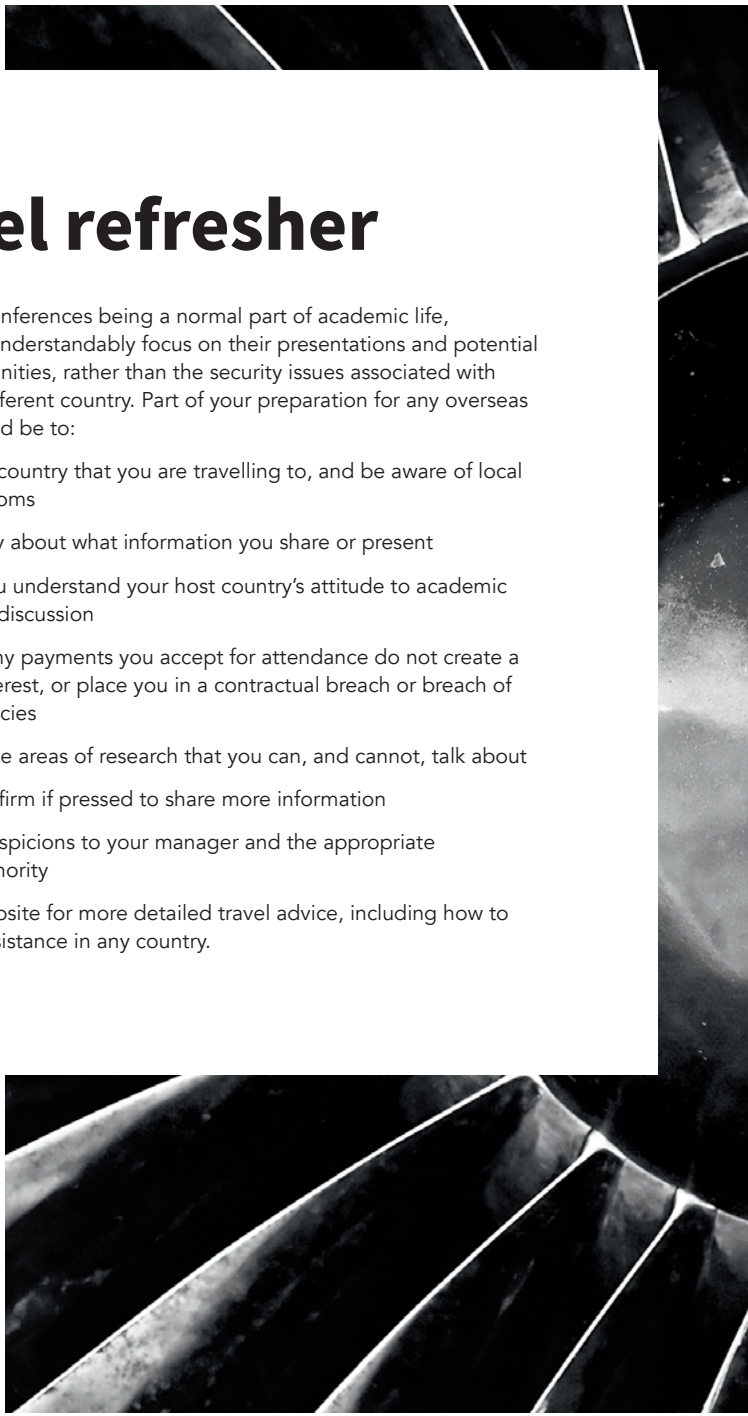
- Public and hotel Wi-Fi connections may not be safe; carefully consider what information you might be sharing when using these connections. Avoid internet banking abroad and implement the guidance above for all other accounts
- Stay alert when using devices and don't share your phone, laptop or USBs with anyone
- Be cautious with any IT-related gifts such as USB sticks. It is safer not to plug them in and to discreetly dispose of them
- Keep your devices with you at all times if possible, rather than leaving them unattended. Hotel rooms, safes and lockers are not always secure because other people may have access codes or keys. However, in these circumstances, encryption helps to keep your data safe

Travel refresher

With overseas conferences being a normal part of academic life, researchers will understandably focus on their presentations and potential research opportunities, rather than the security issues associated with travelling to a different country. Part of your preparation for any overseas conference should be to:

- Consider the country that you are travelling to, and be aware of local laws and customs
- Think carefully about what information you share or present
- Make sure you understand your host country's attitude to academic freedom and discussion
- Ensure that any payments you accept for attendance do not create a conflict of interest, or place you in a contractual breach or breach of university policies
- Be clear on the areas of research that you can, and cannot, talk about
- Be polite but firm if pressed to share more information
- Report any suspicions to your manager and the appropriate university authority

See the FCO website for more detailed travel advice, including how to seek consular assistance in any country.



FURTHER INFORMATION

Academic Freedom Monitoring Project:
https://www.scholarsatrisk.org/academic-freedom-monitoring-project-index/

FCO Travel advice:
https://www.gov.uk/foreign-travel-advice

ICO Guide to GDPR:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/encryption-and-data-storage/

Intellectual Property Office Countries Guidance:
https://www.gov.uk/government/collections/ip-protection-abroad-country-guides

Two-factor authentication:
https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa

Virtual Private Networks (VPN):
https://www.ncsc.gov.uk/blog-post/introducing-new-guidance-virtual-private-networks-vpns

Cyber Aware:
https://www.ncsc.gov.uk/section/information-for/individuals-families

NCSC Small Business Guide:
https://www.ncsc.gov.uk/collection/small-business-guide

Department for International Trade Export Control Joint Unit (ECJU)

Your Technology Transfer Office, legal department or other relevant supporting corporate services should be able to help with advice on export control issues. ECJU also provides a support point of contact which is able to advise on whether a particular end user is likely to be of concern or not. You can contact the ECJU on 020 7215 4594 or by email on eco.help@trade.gov.uk.


730
TOYOTA