NABS+ Network Plus for Analytical Behavioural Science in Security and Defence

EARLY CAREER RESEARCHER (ECR) SAFETY AND WELLBEING: Advice from the Experts

Mental and emotional wellbeing when researching harmful or distressing content

Advice from Dr Allysa Czerwinsky

Do's and Don't's for supervisors, PIs, and institutions.....2

Do's and Don't's for ECRs and researchers.....3

Physical and digital operational security when conducting research

Advice from Dr Ashton Kingdon

Do's and Don't's for supervisors, PIs, and institutions.....4

Do's and Don't's for ECRs and researchers.....5

Safety and wellbeing when disseminating controversial or sensitive research

Advice from Dr Antonia Vaughan

Do's and Don't's for supervisors, PIs, and institutions.....7

Do's and Don't's for ECRs and researchers.....8

COMING SOON: advice from ECRs and other researchers, and existing resources to help - keep an eye on the NABS+ website for more:

www.crestresearch.ac.uk/nabs

Compiled by the NABS+ ECR Steering Group

Advice from Dr Allysa Czerwinsky

Do's and Don't's for supervisors, PIs, and institutions

DO

Be proactive:

- Discuss with students the potential impacts on wellbeing of a degree or research project, before they begin
- Build in opportunities for support and wellbeing into projects – e.g., avoiding lone working and isolation
- Ensure ECRs are prepared for what they might come across in research (or out of curiosity), which might have short or long term effects on wellbeing – and ensure this is done early, e.g., for undergraduates

Train staff members:

- Ensure there is a consistent approach from PhD supervisors regarding researcher wellbeing, proactive and reactive guidance, and pastoral support
- Train and prepare lecturers and supervisors to spot warning signs, emotional vulnerability, or overload

Set up staff networks for those working in sensitive or emotionally demanding research, to enable peer support and engagement

Provide, recommend, or fund specialised, tailored, therapeutic intervention options, and adequately trained mental health professionals:

- Generic counselling is not suitable for the complexity and potential trauma relevant to this field of research

Increase emphasis on research wellbeing in ethical processes:

- Ensure there is a focus on risk, safety, vulnerability, and wellbeing of researchers in the immediate and longer term – the current focus is more (or exclusively) around research participants
- Ensure this is also in place for staff, as well as students

DON'T

Let responsibility lie with researchers:

- Avoid an atmosphere where the responsibility for researcher wellbeing falls on their own shoulders
- Instead, create sustained institutional responsibility and care for support mechanisms, and encourage frank conversations with researchers about risks and mitigations

Let support be only reactive:

- Instead, be proactive – don't expect or wait for researchers to reach out for support or raise concerns

Advice from Dr Allysa Czerwinsky

Do's and Don't's for ECRs and researchers

DO

Actively ensure you are switching off and practising self-care:

- Take breaks and go offline
- Get outdoors – e.g., nature based activities, hiking
- Get moving – e.g., running, kickboxing, yoga, weightlifting
- Practise mindfulness – e.g., colour walks, nature journaling
- Find social connection – e.g., group exercise classes, time with friends and family
- Engage in creative activities where you make something physical – e.g., baking, sewing, crochet. This can shake off the hopelessness of online discourse, and allows you something to point to where you've made or contributed to something tangible

Apply restrictions to social media usage:

- Consider setting social media apps so that you have to log in each time you open them (to prompt you to think first), or setting time limits on apps
- Consider moving towards an analogue lifestyle – consume physical media

Find kindred spirits:

- Find people whose outlooks you share, and whose work feels like it fits with yours – this takes a level of vulnerability but can be worthwhile
- Engage with ECR networks and support

Be proactive:

- Anticipate the potential impact on your wellbeing before entering the field or a research project – discuss this and mitigations with your supervisors
- Build in opportunities for support and wellbeing from the start – e.g., ensuring you are not working alone

Engage in counselling and therapy, where possible

Consider how much of a 'brand' you want to build

- How accessible or available do you want to be?

DON'T

Go through this alone:

- Instead, share your burden with others, especially other ECRs

Physical and digital operational security when conducting research

Advice from Dr Ashton Kingdon

Do's and Don't's for supervisors, PIs, and institutions

DO

Be aware, and ensure staff and students are aware, of repercussions or considerations of public-facing outputs (e.g., media, publications, documentaries, podcasts, opinion pieces)

- Work with staff/student to negotiate a suitable risk appetite

Be proactive:

- Ensure all staff & students know threat assessment and security team contacts – have a conversation to ensure everyone knows the plan in an emergency
- Establish clear protocols for emergencies and/or doxxing – ensure they know who to contact if threatened or their identity is exposed
- Ensure staff and students have a trusted colleague or supervisor to be a point of contact in a crisis

Provide staff and students with resources they need:

- Provide research devices and funding for burner phones
- Provide reputable, paid for VPNs and other software

Protect staff and students' physical safety:

- Remove office addresses from university directories/websites if requested
- Remove other details (phone numbers, email addresses) if requested
- Revise or consider 'open door' policies
- Warn colleagues not to direct unknown people to staff and students
- Have plan in place for unknown/malicious actors showing up in person

DON'T

Let crisis be the first point that you discuss safety and security with staff and students

- Instead, recognise that threats can be scary and destabilising, making it hard to think clearly in the moment and important to have proactive measures in place

Physical and digital operational security when conducting research

Advice from Dr Ashton Kingdon

Do's and Don't's for ECRs and researchers

DO

Maintain separate identities for research and personal use:

- Ensure there is no overlap in details – this way, even if your research persona details are released, this will not mean you are identified in real life, and can prevent doxxing
- Use a dedicated device for research, if possible – an inexpensive laptop with no personal information on it
- Request that your institution provides this – if they cannot, can you upcycle an old device?
- If a separate device is not possible, create separate user accounts and browsers for research and personal use
- On your research browser: disable extensions, clear cookies & caches, and turn off your location, camera (cover camera too), and microphone
- An ideal example: one device for accessing the dark web (which connects exclusively to a hotspot Wi-Fi), one device for day to day research, and a private device for personal use only
- Be aware some encrypted services (e.g., Telegram) require a legitimate phone number – to avoid using your personal number, consider using a burner phone
- Regularly search your persona's username to see what is publicly available

Ensure your privacy settings are correct on each platform:

- Assume default settings are insufficient – audit the settings on every platform
- Disable 'people you may know' features – these use contact lists, location, and browsing history
- Be aware that Facebook aggressively suggests connections based on minimal data
- Turn off read receipts, last seen timestamps, and online status indicators
- Recognise what information is visible to users vs administrators vs law enforcement

Use a VPN or Tor:

- Use a VPN that is reputable and paid for – free VPNs often log and sell data
- Be aware of what VPNs can and cannot do – they protect you from some sites and not others. They hide your IP address from sites you visit, but your VPN provider can still see the traffic
- VPNs are not foolproof, so learn when Tor is more appropriate – it has stronger anonymity, but can be slower and some sites block it
- Consider Talis OS for high risk work (live operating system that routes all traffic through Tor)

If you're worried about institutions or ISPs thinking you're doing something suspicious:

- Consider using a data hotspot instead of institutional network, as the institutional network might log traffic (i.e., that you are using Tor)
- Consider using bridges or obfuscated servers (which disguise Tor traffic to make it look like normal internet activity) if you're worried about your ISP detecting Tor usage

Be careful with what you share publicly:

- Strip metadata from files like photos and documents before posting, for example with ExifTool – metadata can reveal identifying details about your location or device (or other details that can be cross referenced with other information)
- Be careful with screenshots – check nothing identifiable is visible e.g., taskbars, notifications, or images/reflections
- Vary when you post and avoid phrases you typically use – your writing style, vocabulary, and times you post can be used to identify you

Be aware of other publicly-available information about you:

- Beware that if you are asked to speak at an event, it is likely to be advertised – you may not have control over this
- If you can, consider advertising through internal channels only
- If suitable, request details are removed from publications about the event – e.g., your name, photo, livestreaming, or description of the research topic
- Consider using a different publication name to your real family name

Be aware of ethical restrictions:

- Be aware of institutional ethical requirements on deception – this might prohibit you from building completely separate personas with no biological overlap. There are ways around this e.g., using part of your name (surname and middle name)
- Be aware of your own ethical restrictions – e.g., if extremist communities vet new members with a test, proof of identity, or proof of commitment, is it ethical or proportionate to do so, or better to stay on the periphery?

Remember your backstory:

- If you are doing ethnographic research and participating in an extremist environment, remember your backstory –document details securely to avoid contradiction
- Create backstories that are believable but generic enough to remember

Document everything:

- Document and let your institution know the steps you've taken for operational security
- Keep evidence of any threats and harassment – e.g., screenshots, saved messages, recordings (if safe)

Consider your risk appetite:

- Consider how safety measures might affect your career 'impact' – e.g., avoiding interviews, documentaries, media, podcasts, outlets like 'The Conversation', or publications under your real name

Protect your physical safety:

- Minimise public-facing information – office numbers, phone numbers, email addresses
- Consider removing office addresses from university directories/websites
- Beware of 'open door' policies
- Warn colleagues not to direct unknown people to you

Be prepared for what you will do in an emergency:

- Establish a clear protocol with your institution for emergencies – ensure you know who to contact if threatened or your identity is exposed, what you will document, and whether you will report to the police
- Know your institution's threat assessment and security team contacts – have a conversation so that everyone knows the plan in an emergency
- Plan for temporary relocation if threats escalate
- Consider how you will respond to doxxing – will you scrub your online presence, ignore the doxxing, address it publicly, or shut down your online presence completely?
- Recognise that threats can be scary and destabilising, making it hard to think clearly in the moment and important to have proactive measures in place
- Identify a trusted colleague or supervisor to be point of contact in a crisis – ECR networks are useful

Familiarise yourself:

- Know your rights regarding police protection and restraining orders in your jurisdiction – don't rely on your institution to tell you
- Understand common doxxing techniques to help mitigate against them – e.g., reverse image searching, IP logging, cross-platform account linking, social engineering, data breach lookups, and pattern analysis

Remember this is a job – where the effects of research in this area can be significant and long-lasting

DON'T

Cross-contaminate:

- Never use your real details in research accounts/personas (unless ethical restrictions prohibit this deception, see further details in 'Do's')
- Never re-use usernames, email addresses, or handles across research and personal accounts
- Never log into personal accounts when using research VPN or Tor setups
- Never use your research device for personal logins or activity e.g,. a quick Amazon purchase
- Never use your personal device/account/browser for research activity

Discuss sensitive research details over regular unencrypted email/institutional platforms

- Instead, consider encrypted emails e.g., ProtonMail, Tutanota

Safety and wellbeing when disseminating controversial or sensitive research

Advice from Dr Antonia Vaughan

Do's and Don't's for supervisors, PIs, and institutions

DO

Recognise and act on your duty of care in the face of diverse risks:

- Improve institutional policies and procedures – ensure they are comprehensive, effective, consistent, widely understood, and implemented
- Stand up for and defend the validity of researchers and their research, especially where ECRs do not have the capital or reputation to do so
- Put mechanisms in place to enable ECRs to better leverage reputational capital and connections, to build personal and career resilience against bad faith activity against them

Be proactive:

- Establish clear pathways for if/when researchers encounter harm
- Provide relevant training on handling these issues
- Inform researchers of the risks and available support before encouraging them to conduct potentially harmful or sensitive research
- Discuss, plan, and anticipate risks, and the support that might be necessary to minimise risk, support wellbeing, and enable project success
- Join up the relevant teams involved to leverage expertise and avoid duplicated conversations in emergencies – including supervisors, HR, PR, IT security, physical security, ethics boards, etc.

Provide training for other staff members:

- Target supervisors, doctoral schools, and faculties with training on risks and protection measures, to allow knowledge to trickle down to researchers
- Ensure other staff members are trained and recognise their role in mitigating risk to researchers – e.g., ethics committees, IT, security, HR

Create an environment and working relationship where researchers can talk to you and ask for help:

- Encourage ECRs to share problems and seek support
- Emphasise that flagging harassment will not have negative repercussions for researchers
- Ensure senior management take researchers' concerns seriously

Allow researchers to have ownership over their public profile:

- Gain informed consent before publicising their research – relevant to all information including text content, graphics, and framing
- Allow researchers control over their information that is made public – e.g., headshots, location of offices, email addresses

DON'T

Leave risk mitigations up to individual researchers at the individual level:

- Instead, take proactive and reactive action to protect them

Ask ECRs and researchers what they need from you:

- Instead, be proactive in offering what you can do, and what you are willing to do

Leave it to individual researchers to educate institutions on harassment at the point of crisis:

- This can be unnecessary additional emotional labour

Mandate or automate detailed public-facing researcher profiles:

- Instead, gain informed consent for all information that is made public (see 'Do's')

Pressure researchers to publish to generate impact without understanding, communicating, and mitigating the risks involved

Advice from Dr Antonia Vaughan

Do's and Don't's for ECRs and researchers

DO

Be proactive:

- Consider potential risks and mitigations in advance of publishing
- Discuss, plan, and anticipate risks and support that might be necessary (from you, your institution, and funders) to minimise risk, support wellbeing, and enable project success

Evaluate your individual risk tolerance:

- Not just once – repeat this intermittently
- Consider what level of publicity you are happy with for you and your work
- Consider the costs and benefits for your reputation and wellbeing of each publishing outlet or approach to self-promotion

Conduct workplace/work life risk assessments to reduce, manage, and mitigate risks

Conduct an information vulnerability assessment to be aware of and mitigate vulnerability and exposure due to your online footprint:

- Not just once – repeat this intermittently
- Google yourself beyond the second page – people can cross reference between different sources of information
- Recommend that family do not 'follow' you – they might be less concerned or aware about security and privacy, and harassment might turn to them if they're more accessible
- Check your social media profiles – if your usernames are the same across multiple sites, data brokers can patch these together as the same person
- Go private on the electoral register
- Use GDPR and 'right to be forgotten' protections where necessary and possible
- Be cautious about self-hosted websites and platforms where your research can be tied to your personal details
- Request that data brokers remove information about you and your immediate family – details they have can include home addresses and other residents there

Take cybersecurity seriously:

- Use haveibeenpwned.com
- Use strong passwords and password managers
- Use firewall accounts
- Use VPNs
- Silo your personal and professional accounts and technology

Find allies:

- Identify allies and sources of support at your institution
- Build and engage with networks and communities that support wellbeing

Be honest and reflective with yourself:

- Do what you are comfortable with, walk away if necessary, and recognise a job may not be work sacrificing your wellbeing

DON'T

Go it alone:

- Instead, use your supervisors, institution, and ECR networks to support and protect your reputation and wellbeing

NABS+ (NetworkPlus for Analytical Behavioural Science in security and defence) is funded by UKRI and administered by the Economic and Social Research Council (ESRC Award ES/Z502716/1). The views expressed by the researchers and team members are their own and should not be taken as representative of views held by those who fund NABS+. For more information, visit: *www.crestresearch.ac.uk/nabs*