European Cyber Conflict Research Incubator

Equality, Diversity and Inclusion (EDI) in Cybersecurity Education

James Shires, Max Smeets, Alina Meyer, Beth Whittaker and YuYing Mak

12 August 2024

About Us

ABOUT ECCRI CIC

The European Cyber Conflict Research Incubator CIC (ECCRI CIC) advances the interdisciplinary study of the impact of digital and emerging technologies on global affairs, in Europe and beyond. The Incubator exists to conduct, facilitate and promote research and education on these issues for policymakers, industry, civil society, and the general public.

WHO IS THIS GUIDE FOR?

This guide is primarily for universities and other higher education institutions currently running or thinking of introducing Cybersecurity Seminars in their institution. It is addressed to the Faculty Champions and EDI Champions of these programs. Beyond the Cybersecurity Seminars program, this guide may also be relevant for other organizations involved in practical cybersecurity education.

GRAPHICS AND IMAGES

Images on this site were created with the assistance of Midjourney.

Table of Contents

European Cyber Conflict Research Incubator

About The Authors

James Shires

James Shires is the Co-Director of both the European Cyber Conflict Research Incubator (ECCRI CIC) and the European Cyber Conflict Research Initiative (ECCRI). He has written extensively on issues of cybersecurity and EDI in academic journals and for policy institutions including Chatham House, the Geneva Centre for Security Sector Governance (DCAF), and the UN Institute for Disarmament Research (UNIDIR).

Max Smeets

Max Smeets is the Co-Director of the European Cyber Conflict Research Incubator (ECCRI CIC) and the European Cyber Conflict Research Initiative (ECCRI). He is also a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich.

Alina Meyer

Alina Meyer is an independent consultant with over 22 years of experience in the area of human rights, gender, diversity and social inclusion. A former Canadian diplomat and development practitioner, she has consulted for clients worldwide. She holds an BA from McGill University, a Masters in Human Rights from the London School of Economics and a Masters in Social Anthropology from the University of Oxford.

Beth Whittaker

Beth Whittaker is a former analyst with the European Cyber Conflict Research Incubator (ECCRI CIC). Beth holds a masters in Global Security from the University of Glasgow, in addition to an undergraduate degree in Politics and International Relations from the University of Aberdeen.

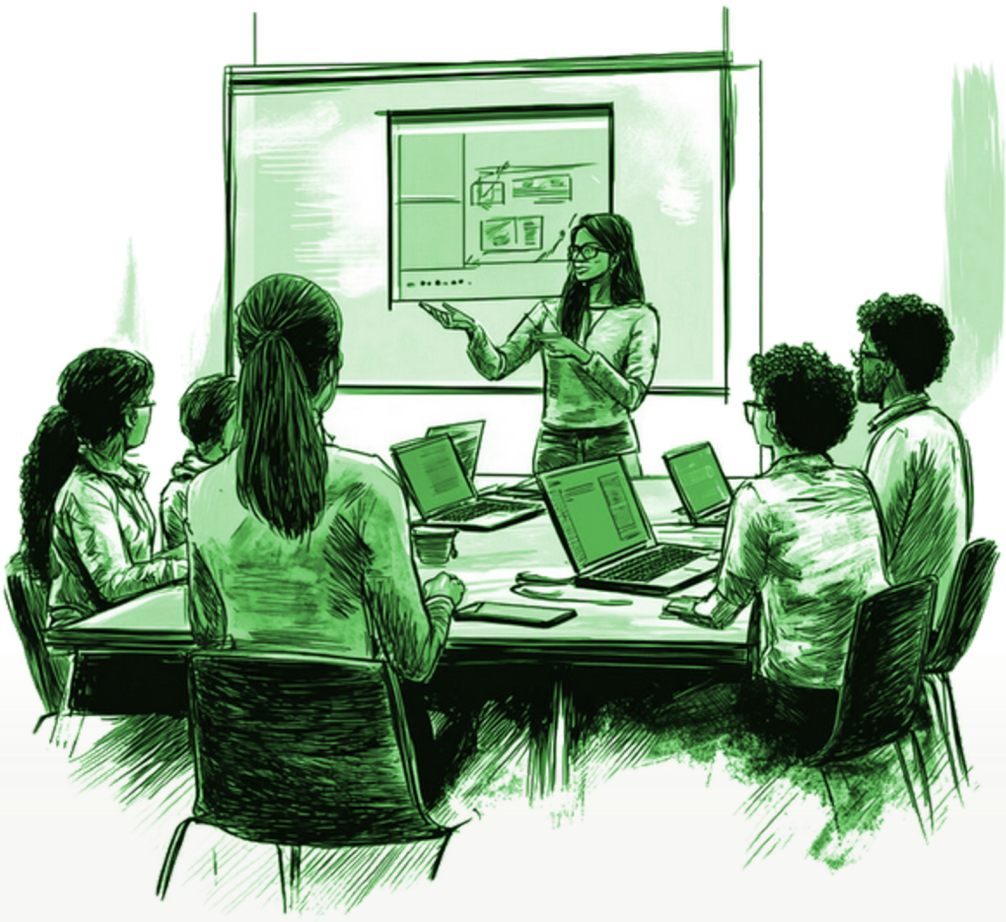
YuYing Mak

YuYing Mak is a Project Officer of the European Cyber Conflict Incubator (ECCRI CIC). She has a Bachelor of Cognitive and Brain Sciences, and attended UWC Adriatic in Italy.

About the Cybersecurity Seminars Program

The Google.org Cybersecurity Seminars program supports cybersecurity seminar courses in selected universities and other eligible higher education institutions in eight European countries, to help students learn more about cybersecurity and explore pathways in the field. The program actively supports the expansion of cybersecurity training in European universities, to build the diverse workforce needed to help the most vulnerable organizations in Europe prevent potential cyberattacks. It also addresses new risks from artificial intelligence (AI), providing students with an understanding of AI-based changes to the cyber threat landscape and helping them effectively integrate AI into practical cybersecurity measures.

Participating universities are expected to actively promote equality, diversity, and inclusion within their programs. They should encourage the strong participation of individuals from diverse backgrounds and create an inclusive environment for education, thereby enriching the overall learning experience and strengthening the cybersecurity community.



Overview

This guide provides an overview of best practices for incorporating equality, diversity, and inclusion (EDI) into practical cybersecurity education, especially the Cybersecurity Seminars program.

We first outline what we mean by EDI, and why EDI matters for cybersecurity education. Not only is an EDI-centered approach the right thing to do, because it supports and advances human rights, but it is also good for educational outcomes.

We then show how EDI considerations are relevant throughout the whole lifecycle of the Cybersecurity Seminars program, and explains how institutions can advance EDI goals without excessive collection of personal data.

We then consider the incorporation of EDI into each step in the Cybersecurity Seminars program in turn:

Step 1	Step 2	Step 3
University Team	**Student Training**	**Local Communities**
Incorporating EDI within the cybersecurity seminars leadership will help build an inclusive environment among faculty and better reflect the field of cybersecurity to students, as well as promoting engagement.	Universities should promote diverse participation in student training, ensuring that learning resources, methods and environments are inclusive and welcoming for all.	Universities should consider EDI when selecting local community organizations for engagement, as well as developing EDI-focused programs for assistance and ensuring sustainability after the program ends.

Overview

Embedding EDI takes time, and sometimes requires additional human and financial resources. We strongly encourage you to take steps towards integrating EDI into as many areas as possible, as soon as possible. By implementing EDI into practical cybersecurity education, you not only improve the learning environment for your students and staff, but also contribute to a better future for the cybersecurity industry.

We include a list of additional resources and an appendix on definitions at the end for further reference.

What is EDI?

EDI is an acronym for Equality, Diversity and Inclusion (also known as DEI).[1] Implementing EDI into university strategies and practices can help promote a representative and inclusive environment for students and faculty.[2]

Equality

Equality ensures that everyone, regardless of their personal characteristics, has access to the same opportunities. You might also come across the term Equity. Equity refers to acknowledging and resolving disproportionate barriers to opportunities and resources that someone might face.

Diversity

Diversity involves recognising and valuing the different backgrounds, experience and knowledge that an individual has.

Inclusion

Inclusion involves creating an environment where people can be themselves, voice and share opinions and where differences between individuals are welcomed and encouraged.

---

[1] DEI often uses the term equity rather than equality, although with a very similar meaning. See the United Nations Global Compact, "Diversity, Equity and Inclusion (DEI)."
[2] Summarized from CIPD (Chartered Institute of Personnel and Development), "Equality, Diversity and Inclusion (EDI) in the Workplace."

What is EDI?

It is important to consider diversity in its widest sense. This goes beyond the usual elements of race, ethnicity, religion, age, ability / disability, and sexual orientation to include factors such as education, socio-economic background, migrant / refugee status, geographic diversity (rural or urban), cultural and linguistic diversity and diversity in terms of ways of thinking and viewing the world, including but not limited to neurodiversity.

> **INTERSECTIONALITY** *recognizes that people's lives are shaped by their identities, relationships and social factors. These combine to create intersecting forms of privilege and oppression depending on a person's context and existing power structures such as patriarchy, ableism, colonialism, imperialism, homophobia and racism.*[3]

Another overarching framework to consider is intersectionality. Intersectionality can be seen as a theory, methodology, paradigm, lens or framework which will help you apply an inclusive element to your work. In essence it is about recognizing the multiple and intersecting identities every person has (such as age, sex, sexual orientation, race, nationality, migrant status, disability, religion, ethnicity, education, poverty status, geographic location (rural / urban), family status, etc.) and how this complexity forms part of a person's lived experience.

[3] United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), "Intersectionality Resource Guide and Toolkit."

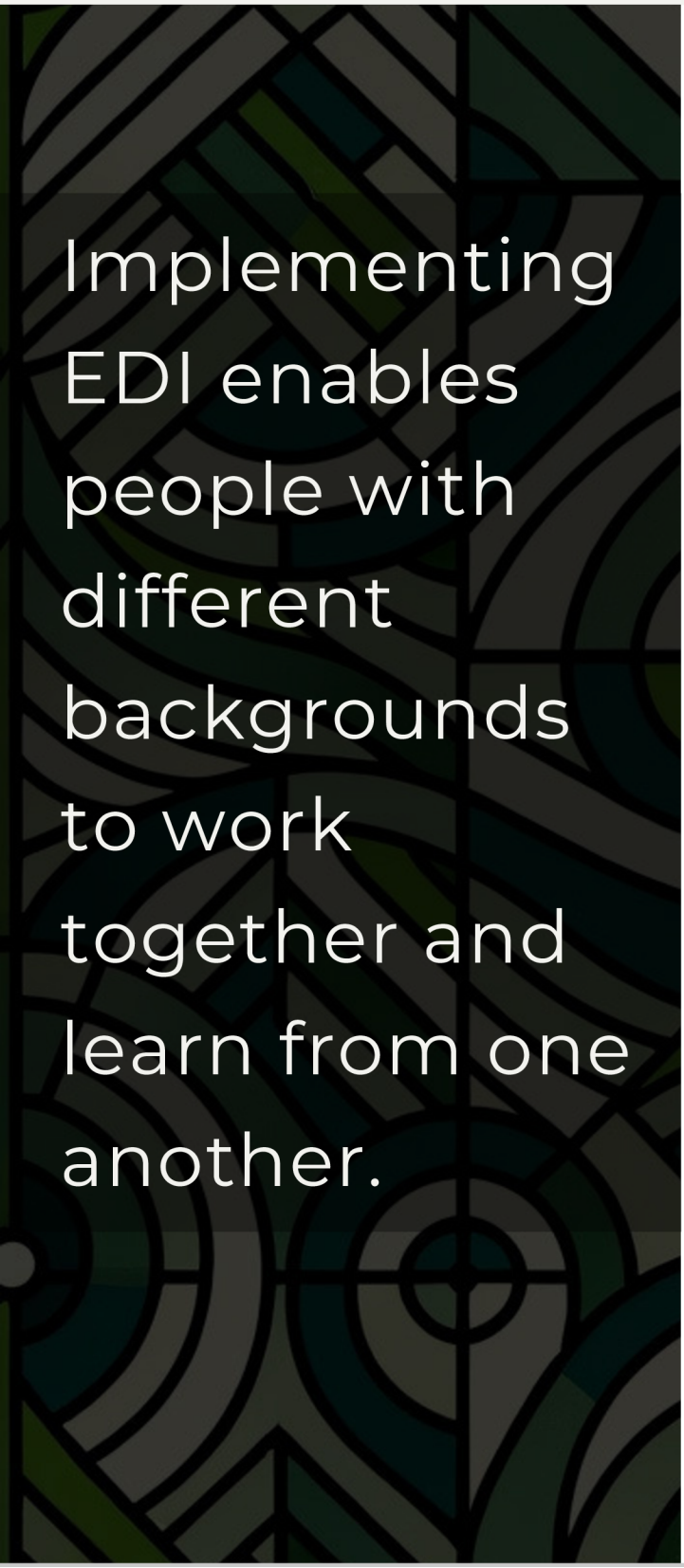
What is EDI?

These multiple identities can compound existing forms of marginalization or discrimination. For example, an elderly, disabled woman living in a remote rural location will have different challenges and possible forms of discrimination than a young, able bodied urban woman, and these different elements of age, ability, sex and geography, among other identity factors combine to form who she is and how she accesses services. It is important that the multiple and overlapping parts of women and men's identities, and a person's identity and relationship to power, are considered in cybersecurity education.

Another related principle is "**do no harm**".[4] Sometimes programs can inadvertently reinforce stereotypes or social or cultural norms and attitudes which reinforce discrimination or inequality. One mitigating strategy is to build a diverse team to design and implement the program.

[4] UK Pact, "Guidance on Gender Equality and Social Inclusion (GESI)."

Why Does EDI Matter?

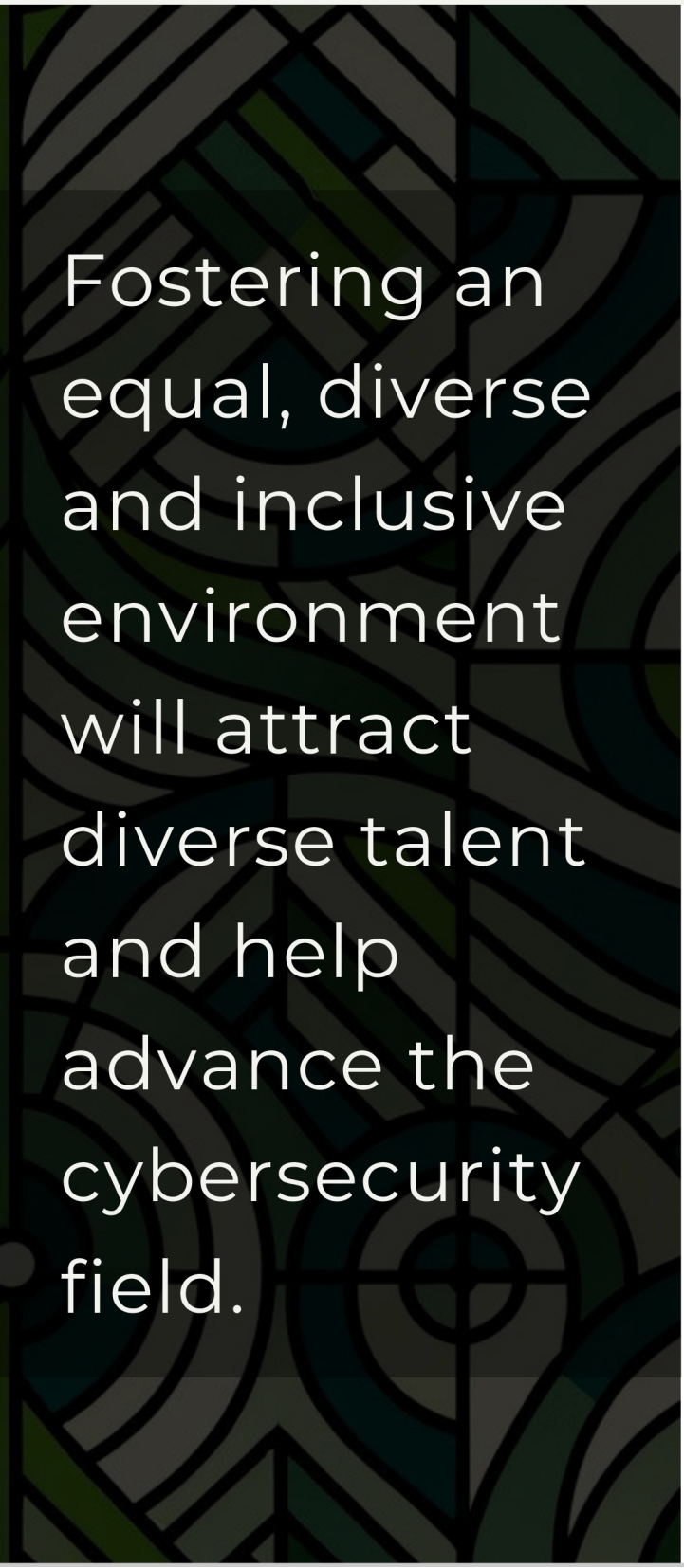


Firstly, EDI is important in and of itself. Implementing EDI into the workplace, and classroom, creates a positive environment where people with different backgrounds can work together and learn from one another. It is beneficial for students and faculty, and aligns with wider societal expectations that the workplace and educational institutions are inclusive.

Secondly, taking proactive measures towards EDI makes organizations and individuals more productive and improves cybersecurity.[5] Not only is an EDI approach the right thing to do, and furthers a human rights-based approach to education, but it is also good for program outcomes and enhances decision making. It has been proven that more diverse organizations perform better and make better decisions. In particular, there is both acceptance and evidence that gender equality promotes better workplace conditions, better decisions, improved productivity, research outcomes and improved policies and governance.

[5] Millar, Shires, and Tropina, "Gender Approaches to Cybersecurity: Design, Defence and Response."

Why Does EDI Matter?



The opposite is also true. A lack of sufficient knowledge and analysis of the challenges and needs of target groups and beneficiaries can lead to the adoption of inappropriate or partial solutions to these problems and needs. It is therefore important to keep EDI considerations at the forefront of educational design to make it more responsive to the needs of all participants, which in turn will create more robust, comprehensive and more sustainable learning.

Ultimately, fostering an equal, diverse and inclusive environment for faculty and students within universities and industry will attract diverse talent and help to advance the cybersecurity field. Creating an inclusive environment at universities improves EDI culture in the future industries students work in, with positive impacts on those industries.[6]

Embedding EDI takes time, and sometimes requires additional human and financial resources. There is no expectation that you will be implementing EDI across all areas of cybersecurity education at all levels. However, we strongly encourage you to take steps towards integrating EDI across as many areas as possible, as soon as possible. By implementing EDI into practical cybersecurity education, you not only improve the learning environment for your students and staff, but also contribute to a better future for the cybersecurity industry.

[6] Hunt et al., "Diversity Matters Even More: The Case for Holistic Impact."

Conducting an EDI Assessment

Conducting a basic EDI assessment (sometimes referred to as a **gender equality and social inclusion (GESI)** assessment) of the content, methodology and approach of your seminars does not have to be costly or timely - it merely involves taking some time to consider the diversity elements of your seminar as well as the logistics of seminar delivery.

Some questions to consider are:

Considerate Scheduling

Is the seminar delivered at a time that is convenient for students / participants to access the seminars?

Caring Responsibilities

If delivery is in person, are there any provisions that can be made for childcare or other caring responsibilities during the seminars?

Physical Access

Will transport, accessibility or safety concerns be a barrier to participation?

Equal Participation

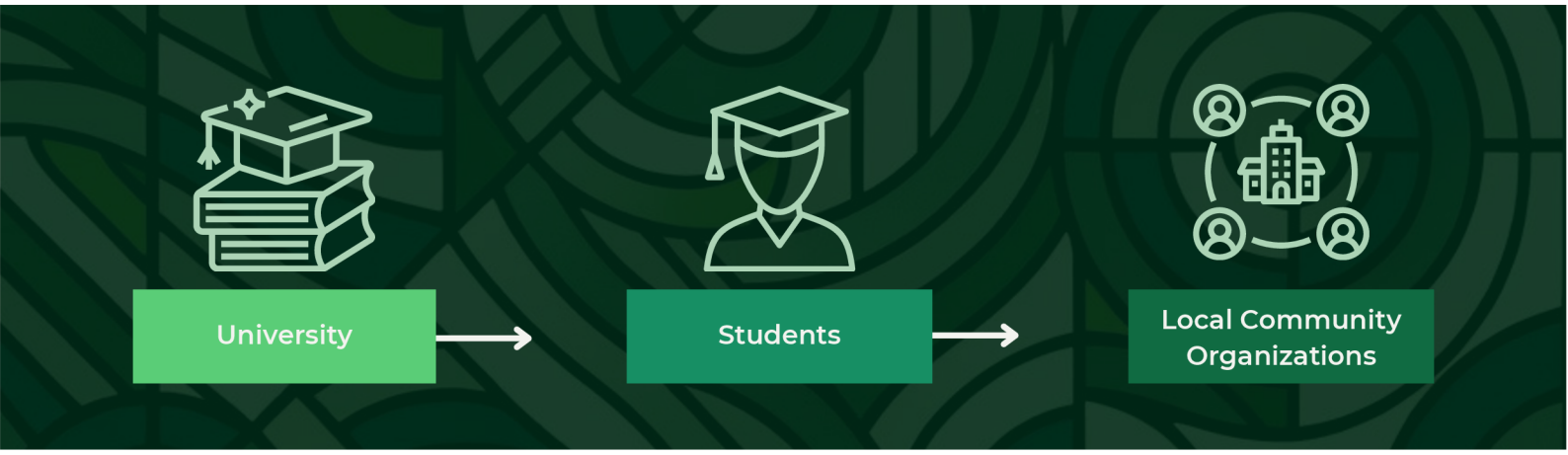
What adjustments are needed to ensure physical or remote access for those with physical, visual or auditory impairments or neurodiverse students who may need adjustments / accommodations?

EDI and Cybersecurity Seminars

Many cybersecurity agencies are already championing EDI. [7] The UK National Cyber Security Centre (NCSC) has conducted pioneering research into diversity in the UK cybersecurity industry. [8] In the EU, ENISA has championed for inclusion and the removal of biases through their #CyberAll campaign. [9] At an educational level, there are numerous university initiatives in related fields. One example is the Rising Stars project, first launched at MIT in 2012, where students from underrepresented groups interested in an academic career within computer science, or electrical engineering, participate in a workshop. [10]

Ensuring an EDI perspective in the early stages of seminar design helps to address more appropriate issues for specific target groups and enables proper planning.

EDI is relevant across the whole lifecycle of a Cybersecurity Seminar (see figure below). First, it is relevant for the faculty and administration of the seminar, including teachers, managers, and instructors. Second, it is relevant for the students participating in seminars, learning from the resources, classes, and activities provided by the university. Third, it is relevant for the local community organizations (LCOs), who receive cybersecurity assistance from those students.



[7] Andrews, "Good Practice Guide for Establishing Equity, Inclusion and Diversity as Part of National Cyber Security Strategy."
[8] Jennings, "Decrypting Diversity: Diversity and Inclusion in Cyber Security."
[9] ENISA European Union Agency for Cybersecurity, "#CyberALL - Embracing Diversity, Empowering Cyber Inclusivity, and Welcoming Fresh Perspectives to Tackle Challenges."
[10] MIT EECS, "Rising Stars in EECS."

EDI and Cybersecurity Seminars

As well as being relevant across all three elements of program design, EDI is simultaneously an individual, organizational and systemic issue:

Individually:

EDI concerns an individual's identity and self-presentation, including their personal perspectives and decisions.

Organizationally:

EDI concerns the policies and practices put in place by institutions, including both those explicitly dealing with EDI considerations and those indirectly affecting them (ranging from harassment and abuse policies to employment contracts and opening hours).

Systemically:

EDI concerns the wider social and national contexts affecting the life chances of individuals, including systemic racism or sexism, population-wide issues such as forced migration, and particular political or cultural touchpoints.

It is important to understand EDI across these categories, as well as how decisions made in one category will inform another. As introduced earlier, the overlapping influence of different aspects of a person's identity on their overall experience of an organization or system is known as **intersectionality**. Through the Cybersecurity Seminars program, you can shape individual and group decisions to better inform students' understanding of the cybersecurity field, whilst making the environment and classroom more diverse.

EDI and Personal Data

You can improve EDI without excessive personal data collection. Consider the following:

Institutional Awareness:

Monitoring EDI progress within your institution is helpful in understanding what is and what is not working.

However, care must be taken over how data is collected and stored to ensure that the institution is abiding by EU or local laws and that the individual(s) who have supplied the data are not at risk.

GDPR Compliance:

Institutions should exercise discretion regarding what equality monitoring data they collect and how they collect it. If the person or institution collecting the data is able to identify the person whose data has been collected, then equality data is considered personal data under the General Data Protection Regulation (GDPR) and is protected.

Anonymization:

Data which is anonymized, that is data which is unidentifiable to the person(s) who it attributes, is not considered personal data by the GDPR. Care must be taken to ensure anonymized data cannot be attributed to the person(s) it relates to.

Equalities Monitoring Policies:

Universities should consult their equalities monitoring policies and relevant legislation to ensure they are complicit with all relevant data protection laws.

Three Steps to Incorporate EDI

The following sections ask **who**, **what** and **how** to incorporate EDI in three key steps:

Step 1: EDI in Your University Team

Who?	Build an inclusive environment among faculty and students.
What?	Construct inclusive seminars with accessible methods and approaches.
How?	Create an open environment to overcome workplace barriers faced by employees and employers.

Step 2: EDI in Student Instruction

Who?	Aim to increase diversity in participation of your seminars and tailor delivery to your target audience.
What?	Consider if your materials are negatively reinforcing stereotypes, language and terminology used, cultural sensitivity, inclusivity and accessibility.
How?	Increase flexibility to accommodate needs of students and staff.

Step 3: EDI and Local Community Organizations (LCOs)

Who?	Prioritize EDI impact when selecting LCOs.
What?	Emphasize a non-hierarchical learning environment and the importance of co-creation with LCOs.
How?	Ensure engagement with LCOs is inclusive for both students and LCOs.

Step 1

EDI in Your University Team

1. Who?

Incorporating EDI within the leadership of the cybersecurity seminars will help build an inclusive environment among faculty, better reflect the field of cybersecurity to students, and will also promote engagement and responsiveness from all students.

Things to consider when forming your team:

Cross-Department Collaboration

The way we think about cybersecurity is changing, and drawing from the expertise you have across other departments can be an excellent way to reflect a broad approach to cybersecurity education. This might include consulting colleagues from a politics department, to expand knowledge of the political consequences of cybersecurity across different environments, the gender studies department, to discuss the gendered implications of this work, the law department to understand policy implications, or the department of Philosophy for practical ethics.

Team Structure

Taking the time to consider the structure of the team, including leadership, teaching, and non-teaching staff, can help to foster an inclusive and open environment. As previously noted, forming a diverse team is beneficial for output. Similarly, encouraging open communication between teaching and non-teaching staff involved in the cybersecurity seminar will help in reporting and responding to feedback and contribute towards a positive and improved work environment.

Step 1

EDI in Your University Team

In addition to this, steps can be taken to embed EDI within the team:

Create Awareness:

Ensure staff understand what EDI is, its purpose and how they can participate in improving the EDI culture.

Build a Vision:

In creating a vision for what EDI will look like among the teaching and non-teaching team, and within teaching materials for students participating in the cybersecurity seminar.

Communicate and Encourage Others:

Find ways to communicate your goals and achievements. This could be done internally among students and staff, or externally on your department's website or social media.

Advertise Cybersecurity Seminars Widely:

Use creative, different methods to ensure they reach a diversity of prospective participants.

2. What?

EDI can be integrated into teaching methods and approaches. When constructing the seminar, you should develop an inclusive and engaging programme for students. For example, the University of Carleton offers a toolkit to incorporate EDI in syllabus and teaching.[11]

This toolkit proposes the following considerations:

- Incorporate **flexibility** into the syllabus structure.
- If your seminar involves assignments, consider using a **variety** of assignment styles to decrease the pressure felt by students for each assignment.
- Have conversations with your students about **workload expectations** at the start of the cybersecurity seminars.
- Have conversations with your students about any **potential barriers** they would face to attending seminars or completing assignments.
- Ensure instructors / trainers have **access** to EDI training and resources.

[11] Harris, Mullally, and Thomson, "Science Is for Everyone: Integrating Equity, Diversity, and Inclusion in Teaching: A Toolkit for Instructors."

Step 1

EDI in Your University Team

You should consider training / sensitization in EDI terminology. For example, all trainers / facilitators should learn the difference between 'gender-sensitive,' 'gender-neutral,' and 'gender-transformative' language to understand how language can perpetuate bias and discrimination. Avoid using harmful stereotypes and gender-discriminatory language that demeans or ignores women, men or gender non-conforming people.

Consider some of the definitions below, and refer to the Appendix for definitions and more detail.

GENDER-SENSITIVE LANGUAGE
ensures gender is appropriately discussed

GENDER-NEUTRAL LANGUAGE
is not gender specific

GENDER TRANSFORMATIVE LANGUAGE
changes biased thinking

3. How?

Creating an inclusive and open environment for members of your team is important for overcoming workplace barriers faced by employees and employers.

Many institutions have adopted flexible working policies, giving members of staff the opportunity to create a schedule which helps maintain their work-life balance and meet their responsibilities away from the office. Flexible working refers to any work arrangement which accommodates flexibility on where, how long and when a member of staff works.

Possible options include:

- Part-time working or job-sharing.
- Flexible start and finish times.
- Remote or hybrid working.
- Compressed work hours.

The options for working arrangements for your employees should be clearly communicated to staff, and available to all. Policies should be clear and easy to understand, so that staff do not feel deterred from choosing flexible working as an option.[12]

Additionally, when on-campus meetings and teaching are taking place, ensure that buildings and rooms are accessible for all team members in attendance. This goes beyond physical access issues to include any auditory, visual, lighting or technological accommodation needed for those with an auditory, visual, linguistic or other impairment or neurodiverse needs.

[12] Ernst Kossek, Gettings, and Mistra, "The Future of Flexibility at Work."

Step 2

EDI in Student Instruction

1. Who?

Students of cybersecurity and related fields reflect the future cybersecurity workforce. A well-known survey by ICS2 reported that women account for only 24% of the cybersecurity workforce, an improvement from 11% in 2017. [13] However, many groups remain underrepresented in the field, with marked intersectional differences. Asian women represent 8% of the workforce, Black women 9% and Hispanic women 4%. Similar numbers are seen in universities.

While gender gaps among students will vary between universities, a study carried out by the UK's Department for Science, Innovation and Technology (DSIT) examining cybersecurity university education found that just 12% of undergraduate students and 23% postgraduate students in cybersecurity identified as female.[14]

> *...just **12%** of undergraduate students and **23%** postgraduate students in cybersecurity identified as female* [14]

[13] "Women in Cybersecurity: Young, Educated and Ready to Take Charge."
[14] Coutinho et al., "Cyber Security Skills in the UK Labour Market 2023."

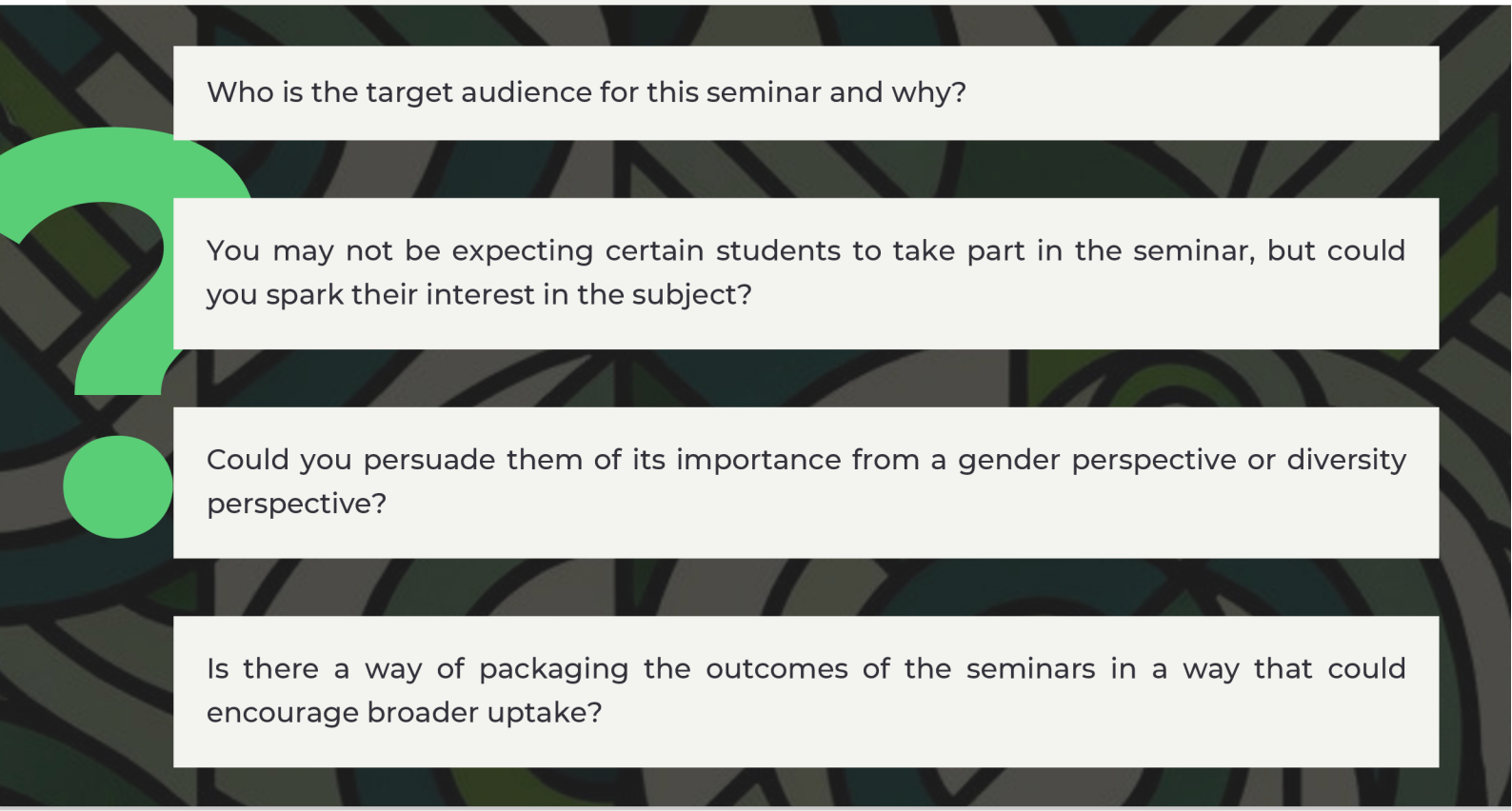
Step 2

EDI in Student Instruction

Many universities and industries are adopting strategies to address these gaps, including outreach to encourage women and girls into STEM generally, or into cybersecurity specifically. An example of this is the Future Advancers of Science and Technology (FAST) programme at the University of California Berkeley, where scientists, technologists, artists, engineers and mathematicians (STEAM) connect with high school students to work on projects and encourage students from diverse backgrounds into STEAM professions. [15]

Diversity in cybersecurity is moving in a positive direction, but more action can be taken to promote diversity among current and future cohorts, as well as to encourage students from a non-technical background to consider cybersecurity as a career option.

Some questions to consider in terms of ensuring diversity of participation in the seminars:



- Who is the target audience for this seminar and why?
- You may not be expecting certain students to take part in the seminar, but could you spark their interest in the subject?
- Could you persuade them of its importance from a gender perspective or diversity perspective?
- Is there a way of packaging the outcomes of the seminars in a way that could encourage broader uptake?

[15] "FAST - Future Advancers of Science & Technology."

Step 2

EDI in Student Instruction

The selection of the right entry points to spark engagement should be a priority consideration for the training team. This result should subsequently inform any necessary change to the training materials and included in the facilitation notes for the training.

Some additional tips for your training team are listed below:

- Use relevant examples to demonstrate the importance of intersectionality.
- Use non-technical analogies to explain technical topics, focusing on their human and / or social impact.
- Explicitly and sensitively ask about and address barriers to participation and involvement.
- Ask for feedback from students, reflect, and respond.

Step 2

EDI in Student Instruction

2. What?

Teaching materials are crucial in establishing and supporting EDI goals, and can help build a diverse and inclusive understanding of cybersecurity among students and staff. Universities should consider carefully the messaging behind what is being taught and the language used.

Some questions to consider when selecting and teaching cybersecurity course materials are:

Do materials negatively reinforce stereotypes?

In course materials and assigned readings, use source materials from authors from different backgrounds to counter stereotypes of who works in the cybersecurity field. When designing your lectures, incorporating diverse images in your lecture slides is a simple way to better represent the cybersecurity field, counter stereotypes, and improve the feeling of EDI in the classroom. Be careful of AI-generated material, as AI-generated content draws from material online, some of which is sexist / biased / gendered. AI-generated content, used without care, can inadvertently reinforce harmful stereotypes and perpetuate discriminatory or harmful content.

Do your topics reflect the breadth of the field?

In addition to technical topics, your cybersecurity seminars could integrate topics which relate to EDI including ethics of cybersecurity, policy implications, and history of the field and influential figures. Other cybersecurity threats could relate directly to EDI characteristics.[16] For example, women (especially of color) face a disproportionate level of harassment and abuse online. Enshrining good safeguarding practices online should be a priority for all cybersecurity education.

[16] ISC2, "Guide to Inclusive Language in Cybersecurity."

Step 2

EDI in Student Instruction

Is the language and terminology inclusive?

Many cybersecurity actors are taking steps to think about and reframe many traditional cybersecurity terms, such as 'Whitelist' and 'Blacklist'. Whitelist is used to refer to something which is 'good', whereas Blacklist is used in reference to something 'bad'. Alternative words you can use instead are Allow List or Block List. For further examples, see the ICS2's guide to inclusive language in cybersecurity.[17]

Language can serve to reinforce or perpetuate existing inequality, discrimination, and power dynamics, hence being conscious of your word choice throughout is critical.

All language in the seminars should be checked with the most up-to-date terminology around EDI. EDI implications of the topics discussed (especially those which might not be obvious to the students) should be added to the seminars curriculum.

Are materials culturally sensitive?

All university staff and instructors / trainers should ensure they are aware of cultural differences and friction points, knowing that EDI discussions can be very sensitive and can stir up discomfort and debate.

Seminars must be tailored to the audience and able to adapt and respond to contextual regional specificities.

[17] ISC2, "Guide to Inclusive Language in Cybersecurity."

Step 2

EDI in Student Instruction

Are materials inclusive?

As mentioned above, inclusion should be interpreted widely, and should include ensuring gender, race and religious diversity as well as diversity of backgrounds and opinions, diversity of age, migrant status, religious or ethnic minority. Emphasize an intersectional approach, taking into account the differing and compounding forms of discrimination faced by marginalized groups. [18]

Are materials accessible?

Depending on the structure of your cybersecurity seminar, you might have students participating with different levels of knowledge. Students can be supported by providing additional background readings appropriate for their level of knowledge, and by contacts of the teaching teams for students if they need additional learning support. Additionally, measures should be taken to ensure students have equal access to course materials, including textbooks, resources and equipment.

This should also include accessibility considerations for those with a disability or neurodiverse students, both groups of whom may require additional accommodations which need to be taken into account and planned for in advance. This pertains to both in-person and online education. Accessibility requirements go beyond physical access provisions such as ramps (for physical accessibility) and should include provisions for sign language interpreters if possible. For online training and web content, ensure the content is also available in a format for people with learning disabilities and in formats that are compatible with software for the visually impaired. [19]

[18] Mowat, "Towards a New Conceptualisation of Marginalisation."
[19] Dunkley, Conway, and Messmer, "Gender, Think-Tanks and International: A Toolkit."

Step 2

EDI in Student Instruction

3. How?

Implementing a flexible method of learning can be a positive way to accommodate the needs of students and teaching staff. A flexible approach to your teaching structure should address three areas: place, pace and mode of study. A flexible structure is beneficial for students, as it allows them to balance work, study, leisure, and childcare or other care commitments, domestic and family duties in a way that suits the needs of each individual.

Here are some tips for fostering EDI in the classroom environment:

- Encourage participation from students, and provide different ways to participate.
- Communicate with students (e.g., give advance warning of deadlines, if possible give course materials ahead of time etc).
- Use non-gendered terms when interacting with students. Additionally, when calling on a student to participate, identify them by a piece of clothing or their position in the room.
- When incorporating peer-to-peer learning in the classroom, designate groups to prevent exclusion. For example, grouping students by asking them to work with the person next to them.
- Provide students with relevant university support or resources. This may include your university's mental health team and learning support.
- Take into account childcare or other care commitments, domestic and family duties, such as elder care or care for a family member with a disability, that some students may have.

Step 3

EDI and Local Community Organizations (LCOs)

1. Who?

The local community organizations (LCOs) you will engage with will vary significantly. Examples may include non-governmental organizations (NGOs), civil society organizations, public service organizations or educational institutions. There is no single solution for how you should choose which LCOs you will assist.

However, you may want to prioritize the following categories:

1. Organizations whose cybersecurity posture does not yet prioritize EDI.
2. Public service organizations with lower levels of cybersecurity maturity.
3. Human rights / gender / civil society organizations with lower levels of cybersecurity maturity.

Step 3

EDI and Local Community Organizations (LCOs)

2. What?

LCO engagement should be inclusive for both students and LCOs. It is important to consider what barriers students might face during LCO engagement, and to provide appropriate assistance and support.

When working with LCOs, be sure to emphasize a non-hierarchical learning environment and the importance of co-creation: ensuring that civil society and the diversity of stakeholders consulted as part of the program have a sense of ownership over the solutions they have identified. The program should apply equitable and accountable partnership principles to ensure that its work with civil society actors does not reinforce power asymmetries. This means that, ideally, LCOs should have opportunities to influence the design of the training material, outreach strategies and engagement approaches. It involves recognising the existing knowledge and capabilities present in LCOs, rather than employing a deficit-based approach to capacity development.

Some tips to help you foster partnerships with LCOs are:

- Ensure students are appropriately equipped with the knowledge of what the LCO does and how to teach others.
- Support the development of relationships amongst LCOs across contexts and regions to foster collective action, including through creating spaces for mutual knowledge sharing and learning.
- Work with ECCRI CIC to track impact in key EDI areas, including particularly the participation of women and other underrepresented groups.

Step 3

EDI and Local Community Organizations (LCOs)

3. How?

Cybersecurity Seminars are designed to assist LCOs with their cybersecurity needs. What this looks like will differ between the design of your cybersecurity seminars, and might include cybersecurity awareness, or vulnerability assessments.

Universities are well placed to help local communities. Student involvement with local communities can be seen in other academic disciplines. Law students at New York University participating in the clinical and advocacy program assist with real-world cases, as do students at universities in the US Consortium of Cybersecurity Clinics.[20][21]

Elements to consider include:

- Build a partnership that addresses the needs of local community organizations, with tailored training plans.
- Ensure consultative and participatory approaches to partnership work, which involve talking to relevant stakeholders, groups, individuals etc prior to the project design and delivery.
- Think of a wide array of beneficiaries reached through the work of the LCO, keeping in mind direct and indirect impacts on these groups.
- Create and share resources for self-teaching.
- Group students appropriately when interacting with businesses.
- Prioritize good, safe and accessible travel options for students, and provide compensation for travel costs where possible.

[20] Sultan, "Improving Cybersecurity Awareness in Underserved Populations."
[21] NYU Law, "Clinics and Externships."

Step 3

EDI and Local Community Organizations (LCOs)

You can best serve LCOs by first understanding what the situation is in your own community; for example, through research or discussions with your LCO network. It is important to remember that each LCO will face different challenges and have different levels of cybersecurity awareness.

The Citizen Lab has compiled a list of good practice examples for inclusive community engagement. [22] Some key practices include being mindful of language used, flexible and open to different methods of communication and engagement, and making sure to reach a diversity of organizations, not just the "usual suspects".

The educational process for LCOs will continue after your student engagement, so ensure your LCOs continue to have access to relevant and up-to-date resources (for example, through maintaining a cybersecurity awareness site).

[22] Fillet, "Inclusive Community Engagement: 10 Good Practices."

Appendix: Glossary and Abbreviations

EDI

Equality

Equality ensures that everyone, regardless of their personal characteristics, has access to the same opportunities. You might also come across the term Equity. Equity refers to acknowledging and resolving disproportionate barriers to opportunities and resources that someone might face.[23]

Diversity

Diversity involves recognising and valuing the different backgrounds, experience and knowledge that an individual has.[24]

Inclusion

Inclusion involves creating an environment where people can be themselves, voice and share opinions and where differences between individuals is welcomed and encouraged.[25]

[23] Summarized from CIPD (Chartered Institute of Personnel and Development), "Equality, Diversity and Inclusion (EDI) in the Workplace."
[24] Ibid.
[25] Ibid.

Appendix: Glossary and Abbreviations

"Do no harm"	Under 'do no harm' principles, an action is conducted in a way that avoids exposing already vulnerable people to additional risks and harms. This is done by actively seeking to mitigate negative impacts and designing interventions accordingly.[26]
Gender equality	The state of being equal in status, rights and opportunities, and of being valued equally, regardless of gender identity and / or expression.[27]
Gender-neutral / blind	Gender-neutral language is not gender-specific.[28] Gender-neutral refers to scenarios, products, innovations, etc. that have neither a positive nor a negative impact when it comes to gender relations.[29]
Gender-nonconforming	A person who is gender-nonconforming does not align with the conventional traits attributed to any gender.[30]
Gender-responsive	Gender responsiveness refers to outcomes that reflect an understanding of gender roles and inequalities and which aim to encourage equal participation and equal and fair distribution of benefits.[31]

[26] Dunkley, Conway, and Messmer, "Gender, Think-Tanks and International: A Toolkit."
[27] "Gender Equality in Research and Innovation Official Development Assistance (ODA)."
[28] Dunkley, Conway, and Messmer, "Gender, Think-Tanks and International: A Toolkit."
[29] Emerson-Keeler, Swali, and Naylor, "Integrating Gender in Cybercrime Capacity-Building: A Toolkit."
[30] Ibid.
[31] "Gender Equality in Research and Innovation Official Development Assistance (ODA)."

Appendix: Glossary and Abbreviations

Gender-sensitive	Gender-sensitive language ensures gender is appropriately discussed.[32] Relating to gender being considered in the research or program but where it is not a central aspect of the research. Gender-sensitive research sets out to ensure, where possible, that it does not perpetuate a damaging gender dynamic, (or is at the very least aware of that damaging dynamic but cannot influence it and must work within it for the sake of the project) or ensure that gender relationships in the context of a specific research project are not made any worse.[33]
Gender transformative	Gender-transformative language changes biased thinking.[34]
Intersectionality	Intersectionality recognizes that people's lives are shaped by their identities, relationships and social factors. These combine to create intersecting forms of privilege and oppression depending on a person's context and existing power structures such as patriarchy, ableism, colonialism, imperialism, homophobia and racism. It is important to remember the transformative potential of intersectionality, which extends beyond merely a focus on the impact of intersecting identities.[35]

[32] Dunkley, Conway, and Messmer, "Gender, Think-Tanks and International: A Toolkit."
[33] "Gender Equality in Research and Innovation Official Development Assistance (ODA)."
[34] Dunkley, Conway, and Messmer, "Gender, Think-Tanks and International: A Toolkit."
[35] "Intersectionality Resource Guide and Toolkit."

Appendix: Glossary and Abbreviations

LCO (abbreviation)	Local Community Organization
NGO (abbreviation)	Non-Governmental Organization
Male-by-default design	Male-by-default design refers to the concept that the default gender – among and for which systems, concepts, ideas, policies and activities have been designed – is 'man'. This is related to androcentrism, which is the practice of centering a masculine world view and marginalizing others. [36]
Non-binary	Non-binary refers to people who do not identify as 'man' or 'woman'. This can also include people who identify with some aspects of the identities that are traditionally associated with men and women. [37]
Safeguarding	Safeguarding is the act, process or practice of protecting people from harm, and the measures in place to enable this protection. [38]

[36] Emerson-Keeler, Swali, and Naylor, "Integrating Gender in Cybercrime Capacity-Building: A Toolkit."
[37] Ibid.
[38] Ibid.

Additional Resources

Andrews, Allie. “Good Practice Guide for Establishing Equity, Inclusion and Diversity as Part of National Cyber Security Strategy.” CREST, January 2023. https://cmage.crest-approved.org/inclusion-and-diversity.pdf.

CIPD (Chartered Institute of Personnel and Development). “Equality, Diversity and Inclusion (EDI) in the Workplace.” Factsheets, November 1, 2022. https://www.cipd.org/uk/knowledge/factsheets/diversity-factsheet/.

Coutinho, Steve, Alex Bollen, Claire Weil, Chloe Sheerin, Dejon Silvera, Ipsos Sam Donaldson, Jade Rosborough, and Perspective Economics. “Cyber Security Skills in the UK Labour Market 2023.” Department for Science, Innovation & Technology (UK), 2023. https://assets.publishing .service.gov.uk/media/64be95f0d4051a00145a91ec/Cyber_security_skills_in_the_UK_labour_ market_2023.pdf.

Department for Science, Innovation and Technology and Department for Business, Energy & Industrial Strategy. “Gender Equality in Research and Innovation Official Development Assistance (ODA).” Department for Science, Innovation and Technology and Department for Business, Energy & Industrial Strategy, May 2021. https://www.gov.uk/government/publicati ons/gender-equality-in-research-and-innovation-official-development-assistance-oda.

Dunkley, Laura, Marissa Conway, and Marion Messmer. “Gender, Think-Tanks and International Affairs: A Toolkit.” Chatham House, February 2021. https://www.chathamhouse.org/sites/default/files/2021-02/2021-02-10-gender-think-tanks-international-affairs-dunkley-et-al_1.pdf.

Emerson-Keeler, Rebecca, Amrit Swali, and Esther Naylor. “Integrating Gender in Cybercrime Capacity-Building: A Toolkit.” Chatham House, July 2023, 45. https://doi.org/https://doi.org/10. 55317/9781784135515.

Additional Resources

ENISA European Union Agency for Cybersecurity. “#CyberALL - Embracing Diversity, Empowering Cyber Inclusivity, and Welcoming Fresh Perspectives to Tackle Challenges.” #CyberALL. Accessed July 10, 2024. Jennings, “Decrypting Diversity: Diversity and Inclusion in Cyber Security.”

Ernst Kossek, Ellen, Patricia Gettings, and Kaumudi Mistra. “The Future of Flexibility at Work.” Harvard Business Review, September 28, 2021. https://hbr.org/2021/09/the-future-of-flexibility-at-work.

FAST. “FAST - Future Advancers of Science & Technology.” Accessed July 10, 2024. https://www.fastprogram.org/.

Fillet, Sören. “Inclusive Community Engagement: 10 Good Practices.” Go Vocal, August 24, 2023. https://www.govocal.com/blog/6-good-practice-examples-for-inclusive-community-eng agement-enuk.

Harris, Candice, Martha Mullally, and Rowan Thomson. “Science Is for Everyone: Integrating Equity, Diversity, and Inclusion in Teaching: A Toolkit for Instructors.” Carleton University. Accessed July 10, 2024. https://science.carleton.ca/wp-content/uploads/EDI_in_Science_Teac hing_Toolkit-5.pdf.

“HRBA Portal: A Human Rights-Based Approach to Programming.” Accessed July 10, 2024. https://hrbaportal.org/.

Hunt, Vivian, Dixon-Fyle Sundiatu, Celia Huber, del Mar Martínez Márquez María, Sara Prince, and Ashley Thomas. “Diversity Matters Even More: The Case for Holistic Impact.” McKinsey & Company, December 5, 2023. https://www.mckinsey.com/featured-insights/diversity-and-inclusion/diversity-matters-even-more-the-case-for-holistic-impact#/.

Additional Resources

ISC2. “Guide to Inclusive Language in Cybersecurity.” ISC2; Chartered Institute of Information Security. Accessed July 10, 2024. https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/dei/DEI-Guide-to-Inclusive-Language-in-Cybersecurity.pdf?rev=862787df9c6f4761acb97bc59cd38530&hash=2C3B15DCDE589109B08B06316DE3EF41.

———. “Women in Cybersecurity: Young, Educated and Ready to Take Charge.” ISC2, 2018. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Women-in-Cybersecurity-Report.pdf?rev=d9c1e6269f8d43b19ee8fae5972a1bf5.

Jennings, Nick. “Decrypting Diversity: Diversity and Inclusion in Cyber Security.” National Cyber Security Centre; KPMG, 2020. https://www.ncsc.gov.uk/files/Decrypting-Diversity-v1.pdf.

Millar, Katharine, James Shires, and Tatiana Tropina. “Gender Approaches to Cybersecurity: Design, Defence and Response.” United Nations Institute for Disarmament Research (UNIDIR), 2021. https://unidir.org/publication/gender-approaches-to-cybersecurity/.

MIT EECS. “Rising Stars in EECS.” Community & Equity, 2024. https://www.eecs.mit.edu/community-equity/rising-stars-in-eecs/.

Mowat, Joan G. “Towards a New Conceptualisation of Marginalisation.” European Educational Research Journal 14, no. 5 (2015): 454–76. https://doi.org/https://doi.org/10.1177/14749041155898 64.

NYU Law. “Clinics and Externships.” NYU | LAW, 2024. https://www.law.nyu.edu/academics/clinics.

Shires, James, Bassant Hassib, and Amrit Swali. “Gendered Hate Speech, Data Breach and State Overreach.” Chatham House, May 2024, 43. https://doi.org/10.55317/9781784135973.

Additional Resources

SIDA. “Human Rights Based Approach to Research.” SIDA, January 2015. https://cdn.sida.se/app/uploads/2021/05/06123132/human-rights-based-approach-research.pdf.

Sultan, Ahmad. “Improving Cybersecurity Awareness in Underserved Populations.” Center for Long-Term Cybersecurity. Accessed July 10, 2024. https://cltc.berkeley.edu/wp-content/uploads/2019/04/CLTC_Underserved_Populations.pdf.

UK Pact. “UK PACT – Guidance on Gender Equality and Social Inclusion (GESI).” UK Pact, April 2021. https://f.hubspotusercontent10.net/hubfs/7376512/cp/general/UK%20PACT%20GESI%2 0Guidance.pdf.

United Nations Entity for Gender Equality and the Empowerment of Women (UN Women). “Intersectionality Resource Guide and Toolkit.” United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), 2021. https://www.unwomen.org/en/digital-library/publications/2022/01/intersectionality-resource-guide-and-toolkit.

United Nations Global Compact. “Diversity, Equity and Inclusion (DEI).” United Nations Global Compact. Accessed July 10, 2024. https://unglobalcompact.org/take-action/action/dei.

European Cyber Conflict Research Incubator

For more information, please visit:

www.cyberseminars.org

If you have any further queries or need to update your contact details, feel free to reach out via email at:

contact@europeancyber.org