Cyber Resilience Badge Benchmark

Overall, a cyber resilience badge should enable children and young people to recognise what matters for staying safe and secure online, developing the skills to react appropriately and recover when threatening situations occur. The activities associated with a badge should enable young people to

- Apply their knowledge of staying safe when using digital to enhance their lives.
- Choose strong passwords when setting up online accounts.
- Keep mobile phones, computers and other devices safe, secure and private.
- Use trusted software and not download apps/programs they are not sure about.
- Explore and use anti-virus software.
- Know when to share decision making with an adult they trust.
- Become aware of their private and personal information and know how to make decisions about what to share.
- Recognise and react to scams, phishing, disinformation and fake news.
- Use social media privacy settings.
- Recognise cyberbullying, grooming and other online exploitation, developing skills to react and recover.

Achieving a badge should be a means of evidencing learning. Where possible it should be identifiable at levels of the SCQF and valued with credit. Such credit could be linked to other certification, for example, the SQA award in Cyber Security Fundamentals, or an SQA Digital Literacy unit at SCQF level 2 to 6.

NOTES
1.The age ranges given are suggested as useful guides in relation to the type of material that would be appropriate for different age ranges. The age ranges deliberately overlap and are suggested as indicative.
2. Relevant learning outcomes from Curriculum for Excellence and, for senior levels, up to SCQF level 6 are included to provide the context of other learning that young people may be involved in through school.
3. The example activities are drawn from key resources sourced as part of a research exercise to identify relevant cyber resilience resources in Scotland and internationally.

Approx age	A cyber resilience badge should enable young people to...	Formal curriculum outcomes and experiences (for comparision)	Example activities
Age 5 - 8	Think about who it is safe to chat to online. Understand that passwords and PINs are personal and should be private. Recognise devices that are connected to the internet. Involve parents/carers in deciding what apps to view/download. Understand why social media apps have age ratings.	Curriculum for Excellence level 1: I can explore and experiment with digital technologies and can use what I learn to support and enhance my learning in different contexts. TCH 1-01a Using digital technologies responsibly I can access, retrieve and use information to support, enrich or extend learning in different contexts. TCH 1-02a I can extend my knowledge of how to use digital technology to communicate with others and I am aware of ways to keep safe and secure. TCH 1-03a https://education.gov.scot/Documents/Technologies-es-os.pdf CfE all levels As I explore the rights to which I and others are entitled, I am able to exercise these rights appropriately and accept the responsibilities that go with them. I show respect for the rights of others. HWB 0-09a / HWB 1-09a / HWB 2-09a / HWB 3-09a / HWB 4-09a https://education.gov.scot/Documents/hwb-across-learning-eo.pdf	Craft activity: Design a safe using cardboard https://start.paloaltonetworks.com/cyber-aces.html Play a game in a group. For example, a game involving passwords. (SWEBOTS activity 9) Follow supplied links to watch relevant video content. For example: https://www.missingkids.org/netsmartz/videos Take part in an activity or discussion with parent/carer. Report back to group on learning. For example https://members.scouts.org.uk/supportresources/4282/digital-citizen-staged-activity-badge
Age 8 - 11	Keep digital devices, software and apps secure with a secure password, PIN, fingerprint etc. Understand why some data should be kept private when setting up online	I can extend and enhance my knowledge of digital technologies to collect, analyse ideas, relevant information and organise these in an appropriate way. TCH 2-01a I can use digital technologies to search, access and	Craft: Build a computer out of junk https://members.scouts.org.uk/documents/6to25/DigitalResources/Digital%20Citizen%20Stage%201%20(criteria%201)%20Build%20a%20crafty%20computer%20Final%20PDF.pdf

Approx age	A cyber resilience badge should enable young people to...	Formal curriculum outcomes and experiences (for comparision)	Example activities
	profiles.

Develop skills to set up online profiles.

Develop appropriate behaviour for online gaming.

Involve an adult they trust in decisions about visiting a website or downloading an app.

Recognise that not all social media content is safe or reliable and know how to react.

Begin to connect knowledge and skills about cyber resilience with opportunities for careers. | retrieve information and am aware that not all of this information will be credible. TCH 02-02a

I can explore online communities demonstrating an understanding of responsible digital behaviour and I'm aware of how to keep myself safe and secure. TCH 2-03a

https://education.gov.scot/Documents/Technologies-es-os.pdf

CfE all levels (Health and wellbeing)

As I explore the rights to which I and others are entitled, I am able to exercise these rights appropriately and accept the responsibilities that go with them. I show respect for the rights of others. HWB 0-09a / HWB 1-09a / HWB 2-09a / HWB 3-09a / HWB 4-09a

https://education.gov.scot/Documents/hwb-across-learning-eo.pdf | Play a Game: Yes – no – maybe https://www.scouts.org.uk/activities/yes-no-maybe/

Create a trail for an activity that is just like a digital footprint https://www.scouts.org.uk/activities/on-the-spot/

Take part in a conversation or activity with parents – for example around age ratings from social media and report back to the group.

https://start.paloaltonetworks.com/cyber-aces.html |
| Age 11 - 14 | Use strong and unique passwords effectively.

Understand and use two factor authentication on email accounts.

Recognise and react to risks from hackers and malware.

Understand benefits of anti-virus software.

Consider appropriate behaviour for | CfE all levels

As I explore the rights to which I and others are entitled, I am able to exercise these rights appropriately and accept the responsibilities that go with them. I show respect for the rights of others. HWB 0-09a / HWB 1-09a / HWB 2-09a / HWB 3-09a / HWB 4-09a

https://education.gov.scot/Documents/hwb-across-learning-eo.pdf

SCQF level 3 Interpret cyber security processes that keep self and others safe and secure when | Complete a digital activity and demonstrate that you have considered relevant cyber resilence aspects. For example, a coding project, a digital collage or photo story.

Play a game about developing strong and unique passwords. Eg https://www.youthlinkscotland.org/develop/developing-knowledge/digital-youth-work/safe-secure-empowered/passwords/

Use scenarios to evaluate social media activity. Eg Digital detectives https://www.scouts.org.uk/activities/digital-detectives/ |

Approx age	A cyber resilience badge should enable young people to...	Formal curriculum outcomes and experiences (for comparision)	Example activities
	peer-to-peer interactions online. Use social media privacy settings to reduce the risk when using these platforms. Know about the Digital 5 Rights 1. The right to remove 2. The right to know 3. The right to safety and support 4. The right to informed and conscious choices 5. The right to digital literacy https://young.scot/get-informed/national/do-you-know-your-digital-rights Explore skills for cyber resilience and opportunities for careers.	engaging in tasks online. Performance criteria 1. Summarise security features used to access and protect devices, data, networks and systems. 2. Explain safe and legal file and information sharing practices. 3. Discuss implications of national laws and regulations relating to cyber security. 4. Explain how a personal digital footprint is created. (National unit specification: Digital Literacy (SCQF level 3) https://www.sqa.org.uk/sqa/files/nq/J3H643.pdf) https://blogs.gov.scot/cyber-resilience/2020/01/29/how-sqa-digital-literacy-units-contribute-to-cyber-skills-development/	
Age 14 - 18	Explore and understand the long term impact of a digital footprint. Use a password manager to generate strong passwords and manage their password use effectively. Apply social media settings skillfully to keep themselves safe and secure. React to and recover from scams, phishing, disinformation and fake news. Use anti-virus software.	SCQF Level 5 Evaluate cyber security skills that keep self and others safe and secure when working and communicating online. Performance criteria 1. Review cyber security features, tools and methods used to protect devices, data, networks and systems from risk and unauthorised exploitation. 2. Locate, refine, assess, organise, store and share digital information with others using a range of appropriate digital devices and tools safely and securely. 3. Compare current international laws and	Complete activities to demonstrate understanding of encryption Encryption https://start.paloaltonetworks.com/cyber-aces.html Create a plan of the Internet of Things in your home and use as the basis for a discussion around cyber risks and security. SWEBOTS Activity 8 Take part in the phishing quiz https://phishingquiz.withgoogle.com/ Take part in a Cyber Security challenge https://www.cybersecuritychallenge.org.uk/what-we-do Take part in a discussion what to do if you are being bullied online

Approx age	A cyber resilience badge should enable young people to...	Formal curriculum outcomes and experiences (for comparision)	Example activities
	Apply the Digital 5 Rights to their online activity. 1. The right to remove 2. The right to know 3. The right to safety and support 4. The right to informed and conscious choices 5. The right to digital literacy https://young.scot/get-informed/national/do-you-know-your-digital-rights Know how to react to cyberbullying, grooming and other online exploitation. Know how to report cybercrime and how to block people from social media. Develop cyber resilience skills and discover opportunities for careers.	regulations relating to cyber security and data privacy. 4. Review and refine a personal digital footprint. (National Unit Specification, Digital Literacy SCQF level 5 https://www.sqa.org.uk/sqa/files/nq/J3H645.pdf) SCQF Level 6 *Level 6: Outcome 1* Critically review cyber security skills that keep self and others safe and secure when working and communicating online. *Performance criteria* 1. Evaluate cyber security features, tools and methods used to protect devices, data, networks and systems from risk and unauthorised exploitation. 2. Locate, refine, assess, organise, store, share and publish digital information with others using a range of appropriate digital devices and tools safely and securely. 3. Evaluate current international laws and regulations relating to cyber security and data privacy. 4. Evaluate digital footprints. National Unit Specification: Digital Literacy SCQF level 6 https://www.sqa.org.uk/sqa/files/nq/J3H646.pdf	https://young.scot/get-informed/national/what-can-i-do-if-im-being-bullied-online Explore https://young.scot/campaigns/national/digiknow for careers information and activities

Resources

The example ideas above are just that – examples – and are not intended to be comprehensive. Some of the examples will be relevant for other age ranges. Those included are mainly drawn from:

https://www.scouts.org.uk/supporters/nominet/
https://start.paloaltonetworks.com/cyber-aces.html
https://www.girlguidingsouthwest.co.uk/swebots-stem-resources/product/swebots-on-the-net-resource-pack
https://www.youthlinkscotland.org/develop/developing-knowledge/digital-youth-work/safe-secure-empowered/

YouthLink Scotland
April 2021

The development of this benchmark was funded by Scottish Government.