Youth Work and Cyber Resilience
What Young People Said

January–April 2024

digital
YOUTH WORK

YouthLink Scotland

Youth Work and Cyber Resilience What Young People Said

Contents

YouthLink Scotland

Young people talk about Cyber Resilience

Young people in four youth work focus groups share about the issues that they face in their online lives.

A project led by Youthlink Scotland asked four groups of young people from different parts of Scotland to explore their understanding of cyber resilience and to think about youth work's role in supporting them.

In the focus group conversations young people identified a range of online safety and cyber resilience issues affecting them and people they know:

- **Cyberbullying**
- **Pressure** - to stay connected and share location data
- **Grooming** and **online exploitation**
- **Scamming/phishing**
- **Addiction** to digital activity, including social media and gaming

Read on for more about what they said and the impact it has on their lives. Wherever possible we've included the words of the young people themselves.

The project was led by YouthLink Scotland with invaluable input from the youth work sector and funding from Scottish Government.

Conclusions and recommendations

- The range and seriousness of the issues affecting young people in the digital world shared in the focus groups were significant and often based on personal experience or experience of people they knew. This highlights the need to **ensure that cyber resilience is discussed with young people regularly**.

- Young people discussed the impacts of online bullying, grooming, being accessible 24/7 and the pressures they faced in the online world. **It is essential that young people are able to discuss these issues with someone they can trust and who can help them seek help and support**.

- Young people are accessing digital technology from younger ages and so it is important to **engage with young people on cyber resilience from primary school age**.

- **Cyber resilience** wasn't an easily understood term for young people. They were more likely to understand online safety or staying safe online. **Changing the language we use to talk about this area** with young people would help them to understand the relevance for them.

- **Ensure cyber resilience is engaging for young people** including personal experiences and memorable materials. Games and activities are valuable to gain interest and awareness.

- **Youth workers can play a key role in supporting young people to discuss and understand cyber resilience**. Creating opportunities for conversations is key.

- **Provide opportunities for peer education** so young people can share the messages with other young people.

Today's context:
digital is an integral aspect of young people's lives

Over the last two decades, digital technology has become an ever-greater influencer in our world, with the pace of change only increasing over time.

Digital Youth Work is a response to this growing influence in young people's lives, providing activities, tools and resources that help them navigate their online lives and develop the skills they need to thrive in the digital world. YouthLink Scotland has played an important part in defining digital youth work, with many examples of varied practice in a great many different contexts.

For a young person, digital literacy includes understanding the range of risks they might encounter online, ranging from cyberbullying to identity theft. Digital Youth Work can help young people understand the threats and challenges, avoid negative influences, and provide support around how to react and recover when things do go wrong.

Definitions

Cyber Resilience

The ability to use technology securely, and to respond to and prevent cyber crime.

Online Safety

is being aware of the nature of the possible threats that you could encounter whilst engaging in activity through the Internet, these could be security threats, protecting and managing your personal data, online reputation management, exploitation, and avoiding harmful or illegal content.

From the research it is clear that the young people in the focus groups do not generally separate these two areas, and tend to start from thinking about personal online safety. Youth workers from one group commented that they would like to run the session again with "online safety" as the title, as they had the sense that there would be better engagement.

The Scottish Government's Cyber Resilience Action Plan includes the intention to "Explicity embed cyber resilience throughout our education and lifelong learning system" and specifically "Work with key community learning and development (CLD) partners to further embed cyber resilience learning and skills development in non-formal learning".

Useful Terms

A few terms that we came across and thought might be useful to define
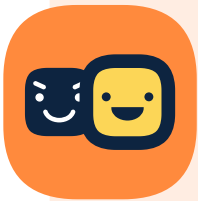
Catfishing

Catfishing refers to the creation of a fictitious online persona, or fake identity (typically on social networking platforms), with the intent of deception, usually to mislead a victim into an online romantic relationship or to commit financial fraud.

Cyberbullying

A form of bullying or harassment using electronic means. Cyberbullying and cyberharassment are also known as **online bullying**.

Doxing

Doxing is the action or process of searching for and publishing private or identifying information about a particular individual on the internet, typically with malicious intent.

Internet safety

Also known as **online safety**, **cyber safety** and **electronic safety** (**e-safety**), refers to the policies, practices and processes that reduce the harms to people that are enabled by the (mis)use of information technology.

Phishing

Phishing is a play on the word "fishing". It is when a cyber-criminal contacts you out of the blue and convinces you to hand over your personal information or money or gets you to download a virus that infects your computer.

How we went about the research

The principles of youth work make clear that youth work is an equal partnership between youth workers and young people, that young people choose to participate and that it builds from where they are. With this in mind, the decision was made to use a participatory research methodology where youth workers were trained to run focus groups with young people. This provided youth workers with an opportunity to develop research skills as well as a chance to facilitate a discussion with young people about cyber resilience. In turn young people were given the opportunity to discuss these issues with skilled youth workers who they trusted and felt comfortable with.

Focus group training

Youth workers were trained online in how to run focus groups using creative methods such as zine making.

The training explored research ethics including how to keep themselves as researchers safe, how to keep the young people safe (physically and emotionally) and how to keep the data safe.

The youth workers were also trained in understanding cyber resilience and online safety.

Running focus groups

Youth workers ran focus groups with young people. In all but one of the focus groups the youth workers worked with the young people they ran the focus group with.

In one of the focus groups, the youth worker is a skilled practitioner and has a national role, so is experienced at visiting groups across Scotland and ran the focus group with a group they did not know. The youth workers were provided with a topic guide for the focus group, consent forms, and information sheets to share with the young people and their parents/guardians.

All focus groups were recorded with consent from the young people and for under 16s their parents/guardians. Youth workers were given clear instructions in how to safely and securely share the audio file with YouthLink Scotland to arrange transcriptions.

Transcribing

YouthLink Scotland arranged for the audio files to be transcribed by an approved and experienced transcriber.

Coding and reflection day

Youth workers were invited to take part in a coding and reflection day facilitated by a Senior Researcher at YouthLink Scotland. On this day the youth workers were provided with a transcript (not from the focus group they ran).

Throughout the day the youth workers were supported and guided in how to code the data (pull out the key themes) and reflect on the key findings that were emerging and to compare the experience of the different focus groups. The following report in based on this coding and further analysis by the Senior Researcher.

Ethics

This project adhered to the ethical principles outlined in [YouthLink Scotland's research ethics policy](#).

The young people who took part in the focus groups

North Ayrshire

6 young people who are all young modern apprentices, aged 16-18, 5 female, 1 male. All working in areas of deprivation and have established relationships with the youth workers who ran the focus group.

Girlguiding – Angus

6 young people all female, aged between 10-15 years. The girls were predominantly from a deprived community. The youth worker who ran the focus group was a volunteer who had an established relationship with the young people.

Girlguiding – Tay and Ochils

7 young people all female, aged between 11-14. All of the young people lived in rural areas, some lived in areas of deprivation and some had learning difficulties. The youth worker who ran the focus group has a national remit, is an experienced practitioner and did not know the young people they ran the focus group with.

Highlands

4 young people including 1 male, 1 female and 2 who preferred not to share their gender, aged between 18-25 years. All of the young people lived in rural areas. The youth worker who ran the focus group knew the young people who attended.
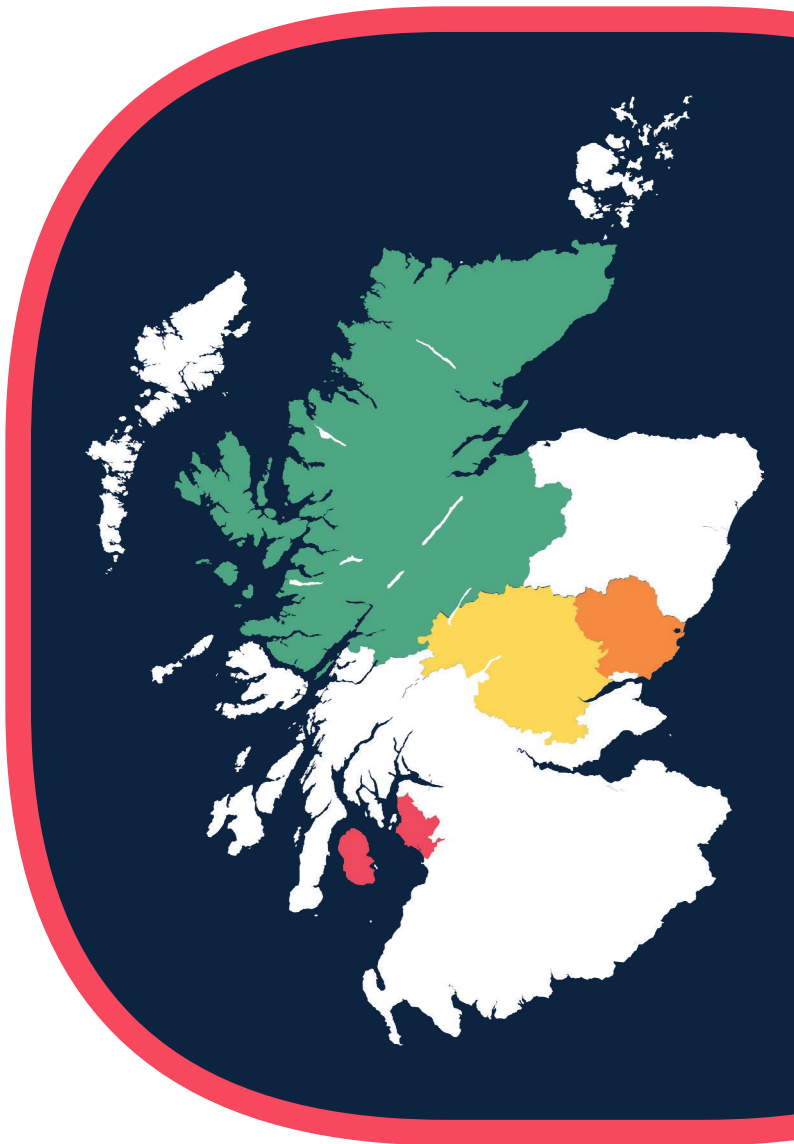
Issues facing young people in the digital world

Young people shared in each of the four focus groups the range and the depths of the issues facing them and their peers in the digital world. There was an acknowledgement across the focus groups about how influential the digital world is in the lives of young people and how much they use digital devices in their day-to-day lives.

> *"I think our generation most of the day we're on our phones"*
>
> **Young Person, Angus Girlguiding**

Cyberbullying is prevalent

Cyberbullying (use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature) was one of the biggest issues identified for young people in the digital world across the focus groups.

For one of the focus groups the young people who were all female, aged between 11-14 and living in rural areas had personal experience of being bullied online

> *"I've been online bullied.*
>
> *I've been online bullied too."*
>
> **Young People, Girlguiding Tay and Ochils**

It manifested for some through name calling, even by people they describe as friends.

> *"Some of the problems I face on the internet... my friend calls me fat and it's not nice."*
>
> **Young People, Girlguiding Tay and Ochils**

There was also an exchange in which the young people discussed how "ugly" photos were being shared online and how the sharing of these photos of them led to them retaliating.

"There's this Snapchat called [Schoolname] Rumours and they message you and they're like sending ugly photos of people or send –

That's really horrible.

And then if you send like...I sent this video to it because I wanted to get added to the private story and then on the private story, they post ugly photos of people and I got posted on it.

That's horrible.

I was on it three times.
But then I found out who posted me on it and then I posted an ugly photo of them on it."

Young People, Girlguiding Tay and Ochils

A form of cyberbullying which was discussed by one of the focus groups was doxing. This is a form of cyberbullying that uses sensitive or secret information, statements, or records for the harassment, exposure, financial harm, or other exploitation of targeted individuals.

"It's like doxing and addresses, like how like... young people first starting out on the internet, having it for the first time, being excited, meeting communities, they might get led into being doxed, like leaking their address out to people and having it –

Sorry what is that word?

Doxing is when your address leaks, it's like people can like know where you live and –

Doxing?

Yeah. Its address leaking, it's just that essentially, it's one that a lot of people fall into and they have to delete things like their accounts when they do leak it and keep themselves safe"

(Young People, Highlands)

Being visible and contactable 24/7

One of the groups of 16-18 year olds, discuss the use of Snapmaps, which is a feature of Snapchat in which it's possible to see live locations of friends.
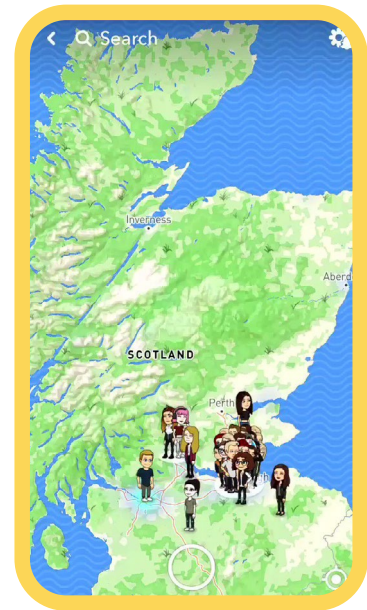
"Snapmaps as well.

Int: *Snapmaps?*

So see when you add someone that means they can automatically see exactly where you are.

And when you're leaving to go anywhere like as soon as you open the Snapchat they can see exactly where you are.

And if you're in a live location –

Or if you're in the car.

If you're in a live location"

Young People, North Ayrshire

Being available 24/7 also means that bullies can contact young people at any time of day too.

&?#!

"Like if you're getting bullied at school or that and then you go home it doesn't stop because people have access to... Also if people are making up rumours about you, they spread much quicker because people can just text their friends and be like oh did you hear that rumour?"

Young Person, Tay and Ochils Girlguiding

Pressure to be online and share personal details

A common theme across the focus groups was young people feeling pressure in the digital world. This pressure exists for young people in different forms and across all ages and genders.

Fear of missing out (FOMO)

This was discussed as fear of missing out and not being in the same online spaces as peers, because if you're "missing out" then you're not "fitting in".

"It's a missing out thing.

FOMO yeah.

Fitting in yeah.

"And that's hard, how do you break that when everybody is…it feels like everybody is in one space"

Young People, Highlands

Being popular

This is explained as the pressure for young people to get a lot of likes/views for content they post on social media as a sign of popularity.

"It's not money and all that, it's now how [many] likes that they have or how many views that they have, it's all about the numbers on their account and stuff and that's also influenced by people who are popular online and all that. So young people are now stressing about…if people have got a lot of likes or something like that which is one of the issues."

Young People, Highlands

Devices listening

There was a concern raised in the Highlands about devices such as Alexa listening and recording exchanges.

"Yeah, so if you go into Alexa search history it listens because obviously its got to listen to you because its got to hear when you say Alexa. So it records snippets so you can listen to the bits that its recorded, it's really interesting actually.

That's quite scary.

Terrifying! It's terrifying!

It's a horrifying thing.

I don't think I'd ever put one of those in my house ever"

Young People, Highlands

Grooming and online exploitation

Young people talked about what it was like to be online, their own experiences and those of family and friends.

There was an issue raised about the vulnerability of young people online and the opportunity for them to be exploited.

"Okay but it's just...like a lot of them, it's the same issue, like them finding a community and getting into it and meeting people on there but like of course they can obviously meet the wrong people and they can take advantage of them by grooming them and/or doing horrible things."

Young Person, Highlands

As part of the Tay and Ochils focus group, a young person under the age of 16 chose to share a personal experience they had of being contacted online by a stranger leading them to experience "panic" and being "scared".

"Even if someone different like a stranger texted you, I've been through a stranger texting me.

Same! It's not nice.

They asked me how old I was. Would I be able to say how old –

I'm 13. They said where was your school at, could I come and see you and I was like no you can't because you don't know where my school is.

....

I nearly had a panic about it because I was so scared. I wanted to speak to the police about it because I was really scared."

Young People, Girlguiding Tay and Ochils

There was a general view expressed about the dangers of being online for young people and the possibilities of strangers reaching young people online and not knowing what or who is real or not.

"Like when the internet wasn't really a thing you could probably just tell your child oh stay away from strangers but now it's not easy because they can even reach you in your own home."

Young Person, Girlguiding Angus

"Yeah, I think that's [social media] probably the biggest apart from TikTok and Snapchat but I feel like a lot of things... I think everything really online is dangerous, anything could be dangerous really because you never really know what's actually real and what's not."

Young Person, North Ayrshire

One concern raised was about the possibility of paedophiles contacting vulnerable young people online and using fake profiles to do this.

> *"And you need to be careful that you do know who you're talking to like especially online because you don't really know the dangers online because anybody could kid on to be anyone.*
>
> *You see it on like movies and stuff. Paedophiles...kid onto be...a young girl and like oh do you want to meet up.*
>
> *When you're young you're just like aye fine you don't actually question it because you're just naïve and young so...and they do go for vulnerable young people because they can sense it. They do tend to go for people that are the easiest to target really."*
>
> **Young Person, North Ayrshire**

Scamming and phishing

Being scammed was a common issue raised by young people in all of the focus groups.

In all of the groups young people could recount stories of themselves, family members and people they know being scammed or attempts to scam them, highlighted in this fairly typical exchange:

> *"Someone scammed her dad.*
>
> *I've been through that too.*
>
> **Int:** *You've had scammers as well?*
>
> *Yeah*
>
> *I've had someone try to scam me today."*
>
> **Young People, Girlguiding Tay and Ochils**

Addiction

In addition to all of the concerns raised by young people in the focus groups about the dangers of the digital world and the potential vulnerabilities, there was also a concern about the addictive nature of being online.

Young people in a rural community likened online addiction to cigarettes.

"It's the same thing with like cigarettes and stuff, when you were in school, in high school at least, you hear all these people saying have you tried cigarettes and stuff and like have you tried it yet, have you tried it yet? No!

But yeah, it's similar to that, I guess. One of those bad addictions, I guess. Its like online stuff is an addiction"

Young People, Highlands

Cyber resilience

Cyber resilience is about keeping data and devices safe and would include passwords and phishing. All of the young people in the focus groups had some knowledge about keeping their data and devices safe, however, not many knew this as cyber resilience.

Young people's understanding of cyber resilience

None of the young people across the focus groups could confidently say when asked that they knew what cyber resilience meant.

Age did not seem to be factor in how much knowledge young people had about cyber resilience, for example the older young people did not appear to know more than the younger. The 16-18 year olds in North Ayrshire did not know what it was. For the young people in Tay and Ochils they focused on the word resilience and the idea of "bouncing back" after experiencing "bad things happening online". The word resilience was also the focus for the older young people from Highlands who thought it meant that when experiencing issues in the digital world "so if you are resilient, I guess that means you don't get affected by those things". Angus young people made a good guess that cyber resilience is about "internet protection...from people trying to...steal your information".

Despite not knowing the exact language of cyber resilience they were all familiar with the behaviours such as phishing and scams. They were also familiar with the protective measures that can be taken such as strong passwords, blocking, face ID, 2 factor authentication. For younger young people (under the ages of 16) they also discussed the controls that their parents have on their devices to help protect them.

There was also some awareness of some more enhanced ways to keep devices safe through ensuring that they have strong passwords. For example, a young person from Angus explained that there is an App to check the strength of passwords.

"Didn't we do this app where it says like it's for children like enter your password to see if it's safe and then if it showed up green well it's safe and then if it showed up in red someone can get that easily."

Young Person, Girlguiding Angus

How cyber resilience affects young people's day-to-day lives

In each of the focus groups young people understood what scamming is and could recall examples of scams they're aware of and for some, close family members who had been affected.

Due to this knowledge of the impact of scams, ensuring that their devices were protected appeared to be a regular if not day-to-day consideration. The main way this was discussed was in protection of passwords. Young people in Angus were particularly concerned about their friends not having access to their passwords.

"It's because when friends come over, they ask for our Wi-Fi because our Wi-Fi is not that strong...but I know the password so I don't tell them but like I ask them to hand over the phones and stick in the Wi-Fi password for them."

Young Person, Girlguiding Angus

Parents seem to play an important role in educating young people in cyber resilience and helping them to stay safe.

"My mum put this thing on my phone where basically I can't get apps, she has to sign in."

Young Person, Girlguiding Angus

Some of the young people from North Ayrshire seemed to be particularly concerned about the impact that not being cautious enough with sharing phone numbers, passwords etc could have on their families.

> *"That's just reminded me about something when I was out playing in parks and all that when I was a wee wean I used to...my phone died, I gave my pal my mum and dad's phone number to phone them and say I'll be home about this time... that's really no' the best idea when I look back on it but they were my pals but now I don't speak to them so they still have my mum and dad's number, they could do anything with that. That's just...I cannae get it off them noo can I?"*
>
> **Young Person, North Ayrshire**

> *"So if somebody is getting on your phone and getting your elderly grandparents and stuffs numbers who might then fall for like a scam and stuff like that, it's just about keeping stuff like that safe."*
>
> **Young Person, North Ayrshire**

There was an understanding about not sharing passwords with anyone including friends.

> *"You know when like your friends find out your phone number. Not like your phone number but your password because my friend somehow guessed my password before, it was quite simple but it was easy to remember but I immediately changed it and they kept on trying to find out my new password."*
>
> **Young Person, Girlguiding Angus**

Where young people have learned about cyber re-silience

Once the young people understood what was meant by cyber resilience, they could identify where they had learned about it, though it was more likely to be referred to as online safety or being safe online.

School, Cadets and drama classes were all places where young people had learned about cyber resilience.

> *"That was where I learn what phishing was [computer science at school] and all that, all the terms, I'd heard about it from all the mistakes that my parents made. [Laughter]"*
>
> **Young Person, Highlands**

In the Guides they have an opportunity to work towards a cyber resilience badge, though it was not clear if any of the Guides in the focus group had.

There was general consensus that young people should be taught about cyber resilience from an earlier age. The Angus young people shared that "a lot of people in our class already had phones in P5". This view was shared by young people in the Highlands, who felt that waiting to teach young people about cyber resilience in secondary school was too late as they already have their own devices in primary school, as shown in this extract.

> *"I think from primary school age it should be taught.*

> *Yeah 100% and it's not sometimes, it's like late academy it's taught and not primary school and that's like –*

> *It's too late.*

> *Yeah. Yeah.*

> *By the time the kid gets to the academy they've already got their own phone.*

> *Oh yeah, before that, before that.*

> *And a Snapchat account."*
>
> **Young People, Highlands**

The youth work role

Youth workers can have important conversations with young people, helping them explore cyber resilience

All of the focus groups took place with established groups of young people who knew and trusted each other.

Within the context of these established groups, young people were in agreement that youth work had a role to play in helping young people understand cyber resilience, as well as in schools and by parents/guardians. For young people attending Guides, it was important to have an opportunity to talk about cyber resilience, as one young person shared.

> *"Just talking to us more about it. They can't really do anything physically but like they can still warn us about it and that will make us more self-aware."*
>
> **Young Person, Angus Girlguiding**

It was shared by a young person in North Ayrshire that young people may feel more comfortable speaking to a youth worker than other adults in their life about cyber resilience.

> *"I think a lot of young people if they spend time with youth workers and stuff like that, they might feel more comfortable speaking to like a youth worker rather than like an adult maybe at home. So like as a youth worker is probably like your job to like reinstall the safety of online and like cyber stuff as well."*
>
> **Young Person, North Ayrshire**

Engaging in appropriate settings

It was also highlighted about the need to ensure that learning about cyber resilience is not "boring", perhaps through use of games where they would be more likely to remember the messaging "a game would stick in your mind though as well".

> *"I understand that you have to educate people to be safe online but it's kind of boring if you're just sat there for 40 minutes listening to someone yap about why you shouldn't get Snapchat or something."*
>
> **Young Person, Girlguiding Tay and Ochils**

Despite wanting cyber resilience to be engaging, for some young people the messages need to be shared in appropriate settings and is not the responsibility of every youth group, for example sporting clubs.

> *"I don't think its football's responsibility to be like guys stay safe online."*
>
> **Young People, Girlguiding Tay and Ochils**

"We can teach other people"

Young people can also help teach others about cyber resilience and issues they may encounter online.

This was a point raised by a young person aged 10-15 in Angus.

"And then we can teach other people."

Young Person, Girlguiding Angus

It was also discussed by the young apprentice youth workers in North Ayrshire, one of the apprentices felt young people may listen to them more because they are closer in age.

"I think a lot of the youth workers...a lot of us are younger and more close to their age so maybe they listen to us more if we're telling them the danger of...like obviously an adult they don't really...they don't really know but...and they're just like of saying that to keep them off things but like as us we're younger, nearer their age, they would open their eyes more and listen to us more."

Young Person, North Ayrshire

Sharing experiences

Young people's own experiences are valuable for helping others learn and understand more about cyber resilience.

For young people in North Ayrshire and Highland they felt it is important for personal stories, that young people can relate to, to be shared as part of cyber resilience work.

"Most of us will actually have had a bad experience online, we could even share like what happened to us and say how we could have prevented what happened to us happening to them."

Young Person, North Ayrshire
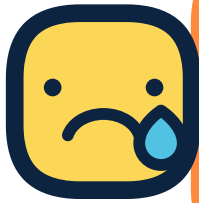
"Maybe like add in like a story of you've had a scary incident yourself in the digital world and say it back to them and be like just be careful if you do that similar thing."

Young Person, Highlands

These stories can be shared by youth workers or young people, there was also a suggestion that the police could talk to young people about their experiences.

"Get the police in to talk about like...their experience and what they've dealt with, to get somebody that's been...had something happen to them, like a personal experience, something that they can relate to."

Young Person, North Ayrshire

"It should be a mandatory thing to do"

There was a view shared by young people in Highland that youth work supporting young people with cyber resilience should be "mandatory" .

"I think all youth groups should be doing this regardless, it should be a mandatory thing to do since it's a youth group and online is a very important thing nowadays that needs to be talked about a lot."
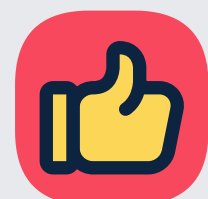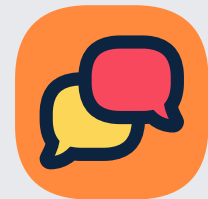
Young Person, Highlands
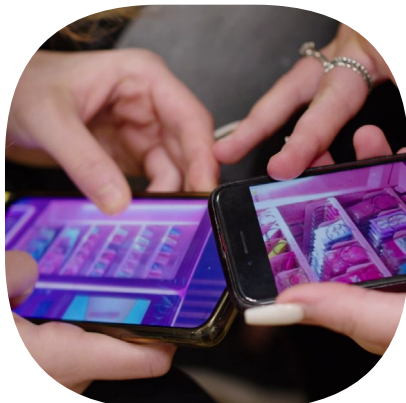
Conclusions and recommendations

We set out to understand what actions youth workers could take and what resources were needed to support them.

Based on what the young people said, our research concluded the following:

- The range and seriousness of the issues affecting young people in the digital world shared in the focus groups were significant and often based on personal experience or experience of people they knew. This highlights the need to **ensure that cyber resilience is discussed with young people regularly**.

- Young people discussed the impacts of online bullying, grooming, being accessible 24/7 and the pressures they faced in the online world. **It is essential that young people are able to discuss these issues with someone they can trust and who can help them seek help and support**.

- It was highlighted that young people are accessing digital technology from younger ages and so it is important to **engage with young people on cyber resilience from primary school age**.

- **Cyber resilience** wasn't an easily understood term for young people. They were more likely to understand online safety or staying safe online. **Changing the language we use to talk about this area** with young people would help them to understand the relevance for them.

- **Ensure cyber resilience is engaging for young people** including personal experiences and memorable materials. Games and activities are valuable to gain interest and awareness.

- **Youth workers can play a key role in supporting young people to discuss and understand cyber resilience**. Creating opportunities for conversations is key.

- **Provide opportunities for peer education** so young people can share the messages with other young people.

digital
YOUTH WORK

This research was supported by funding from the
Cyber Resilience Unit of Scottish Government.

**We would like to thank the young people and the youth
workers from across Scotland who took part in the project.**

Digital Youth Work
digitalyouthwork.scot

YouthLink Scotland
youthlink.scot
info@youthlink.scot

Caledonian Exchange
19A Canning St
Edinburgh
EH3 8EG
Scottish Charity No. SC003923

YouthLink
Scotland

Scottish Government
Riaghaltas na h-Alba
gov.scot