

# Online Resilience Tool







What is digital resilience? Digital resilience is a dynamic personality asset that grows from digital activation i.e. through engaging with appropriate opportunities and challenges online, rather than through avoidance and

safety behaviours. (UK Council for Internet Safety, Digital Resilience Framework, September 2019).

# **Using the Tool**

The Online Resilience Tool is a practical way to assess young people's online behaviour and help you make a decision about whether that behaviour represents risk of harm.

Behaviours are organised by age group and divided into 'Not Harmful', 'Potentially Harmful' and 'Harmful'. The majority of behaviours young people engage in online will fall into the 'Not Harmful' section. There is no way of completely eradicating risk in the online world. In the same way as we cannot completely eradicate it in the offline world, however we can reduce risk through interventions and support which will be discussed at the end of this document.

When using the tool you should always consider the wider context of the young person's life. If the young person is less mature you may want to assess their behaviour based on a lower age group. Equally, if you know certain behaviours are unsafe for a young person, you should use that information to make a safeguarding decision, (for example if a young person has severe body image issues and starts posting a large number of selfies this could be an indicator of a problem). Opposite are explanations of the 'Not Harmful', 'Potentially Harmful' and 'Harmful' categories, followed by the tool and information on how to respond to identified behaviour.



## Not Harmful

These behaviours are normal and can be considered low risk for the young person and people around them. The young person interacts with the online world in a variety of ways whilst also having a range of interests and activities outside of it, including interacting with their peers offline. The young person enjoys the activities they engage in online. As they grow older they will be more private about their online activities; they may increasingly use technology to organise their social lives. Young people may interact with adults through appropriate forums such as online games, but will mainly interact with peers.

For older teenagers some behaviours in this category may conflict with parents' or professionals' values but reflect normal adult behaviours.

Note: Once a behaviour is in the 'Not Harmful' column it will remain in that column for every subsequent age group.

### **Potentially Harmful**

These behaviours may indicate a risk of harm to the young person or someone else.

Potentially harmful behaviours mean you must have a conversation with the young person (or their parent/carer depending on their age) to find out more. Potentially harmful behaviours only show that more information is needed to assess the risk of harm, or actual harm to the young person. Once more information is received you should be able to identify whether the behaviour is harmful or not.

## Harmful

These behaviours represent a high risk of harm to the young person or other young people. The young person may be doing them compulsively and may experience withdrawal symptoms if the behaviour is stopped or curtailed. They may be a victim of intimidating or humiliating treatment online or may be the perpetrator of this, which could include bribery, trickery or threat of violence. The young person is likely to be highly secretive about their online activities, beyond what might be considered a normal desire for privacy.

Any behaviour that involves accessing illegal content is a harmful behaviour.

If you identify a harmful behaviour you will need to act immediately and offer follow up support (see below for suggestions on this).

Note: If you see a behaviour in harmful, it would also be harmful for all younger age groups.

NB: You will not see the term cyberbullying throughout the Online Resilience Tool. We have left it out because any of the behaviours may indicate that bullying is taking place and cyberbullying is not distinct from offline bullying.

Age	Not Harmful	Potentially Harmful	Harmful
Age 0-5 y/o	<ul> <li>Not framful</li> <li>Playing age-appropriate games with a family member (aimed at this age group, consider PEGI rating)</li> <li>Role modeling age-appropriate characters</li> <li>Being aware of/being told there is 'adult content' online</li> <li>Asking to have a photo removed/ not put on social media</li> <li>Watching films/TV with family member</li> <li>Supervised Skyping with remote family members</li> <li>Interacting with a digital device</li> <li>Interest/involvement in family social media e.g. looking at news feed, asking to see pictures</li> <li>Curiosity around digital devices</li> <li>A variety of interactions and responses to devices</li> <li>Being left alone with a device with parental controls in place for up to 10 minutes</li> <li>Talking about how they feel if they see something upsetting</li> <li>Watching a family member play age-appropriate games</li> </ul>	Harmful Gaming alone Preoccupation with digital devices Reaching for a device as soon as they wake up Using screens less than an hour before bedtime	<ul> <li>Watching age-appropriate digital content with friends unsupervised</li> <li>Role-playing or parroting adult content (e.g. sex/ violence)</li> <li>Watching adult content</li> <li>Being left with a tablet/ smartphone unsupervised for 30 minutes or more</li> <li>Upset or aggressive response to withdrawal of device (beyond what is normal for the child)</li> <li>Sexual or violent language</li> <li>Having their own social media account</li> <li>Use of digital devices after bedtime</li> </ul>

Age Not Harmful	Potentially Harmful	Harmful
6-8 y/oAge-appropriate gaming with adult supervisionFilming themselves/friends playing age appropriate gamesGuided research/learningSupervised schoolwork using online technologyMessaging friends on shared 	Being left with a tablet/ smartphone unsupervised for 30 minutes or morePreoccupation with digital devicesGaming aloneMulti-player online gamingSecretive use of online deviceOwnership of their own devicesAccidental access of sexual contentMimicking online behaviourBeing obsessed with selfiesPosing all the timeBeing obsessed with celebrities/wanting to be a celebrityGanging up on or isolating others onlineAccidentally sending selfiesKnowing passwords to parental devicesHaving their own social media accountSharing passwords	Use of digital devices after bedtime Contact with strangers online Sexual or violent language Accessing pornography Sexualised posing Requesting images to be airbrushed Sharing indecent or distressing images with peers

Age	Not Harmful	Potentially Harmful	Harmful
9-12 y/o	Gaming (on or offline) in line with age restrictions	Playing age-restricted games Receiving gifts in online games from family members Watching films/TV online alone	Disrupted sleep through device dependence/gaming
	Doing homework alone		Receiving gifts in online games from strangers (someone unknown to parents)
	Learning how devices work with supervision		
	Learning how to write code with supervision	Use of digital platforms without parents/carer's	Use of digital devices after bedtime
	Looking at social media with friends/family	knowledge Regular social media use	Online gambling Researching issues in an
	Sending friends direct messages	ages Online interaction with strangers Sear losin actively promoting it among peers Usin actively promoting it among peers of subscribers/followers on online cast/social media channels (for example YouTube/Instagram) Sear Sear Sear Sear Sear Sear Sear Sear	unsupported way e.g. self-harm, depression, eating disorders
	Group messaging with friends		Searching for information on
	Sharing things seen online with friends in person		losing weight Using fake social media
Making content and p online	Making content and publishing online		accounts to trick or humiliate others
	Having a private social media account		Sexualised posing online
	Having private direct messages		Sending/receiving nudes/ Sexting
	Posing all the time Using filters on pictures	Being obsessed with celebrities, wanting to be a celebrity	Frequent access to pornography
	Meeting online friends with a parent or carer present	Accessing pornography as a one-off Becoming an influencer/ brand ambassador	Requesting images to be airbrushed
	p		Placing oneself at physical risk in order to take selfies or generate online content
		Knowing passwords to parental devices	Anxiety around digital communications
		Excessively sharing personal information online	Being secretive* about direct messages
		Sharing social media/device passwords with others	Accessing extremist websites
		Taking selfies all the time	Repeating extremist views read about online
		Ganging up on or isolating others online	Accessing illegal content
		Having a public social media account	Online dating Meeting online friends unsupervised

\*Secretive - young people have a right to privacy, and as such may not want to show a parent or carer messages sent to peers. However, sometimes this may go beyond a normal expectation of privacy, for example if a young person becomes very agitated about someone seeing their messages it could be a sign that they are being bullied, groomed or exploited online.

\*\*Compulsive - this is behaviour that is getting in the way of the young person doing what might normally be expected of them, for example if they stop seeing friends, completing school work etc. This differs from excessive behaviour which may still happen very frequently but not to the point that it is interfering with normal activities. In having a conversation with a young person a about excessive behaviour, it is important to determine whether this behaviour is actually compulsive or more of a habit.

Age	Not Harmful	Potentially Harmful	Harmful
13-15 y/o	Learning how devices work Learning how to write software Using reliable sources to find out about personal issues (Brook, Talk to Frank, NHS direct) Posting content on social media Instagram/Snapchat stories One to one messaging and opting to leave or mute a group chat Commenting on a status Accidentally receiving nudes Having a YouTube channel Running Snapchat streaks with friends Blocking and reporting someone for posting inappropriate content Asking to have a photo removed/not put on social media Removing a picture of someone else when asked Having celebrity role models/aspiring to be like a celebrity Private use of digital platforms	Playing older age- restricted games with parental consent Searching for information on losing weight Writing a blog Use of digital devices after bedtime Preoccupation with selfies Excessive posing Requesting images to be airbrushed Sharing social media/ device passwords with others Being secretive* about direct messages Ganging up on or isolating others online Fear of missing out leading to separation anxiety from social media Setting up a fake social media account to explore gender identity or sexuality Regular use of pornography Online dating with peers Sending/receiving nudes/ Sexting Accessing deep web*** sites using browsers such as Tor to explore what is there	Disrupted sleep through device dependence/gamingOnline gamblingUsing unreliable sites to find out about personal issuesAccessing pro-self-harm or pro-ana (pro-anorexia) sitesPassive social media use i.e just scrolling, never commenting or messagingSetting up a fake social media account/ pretending to be someone else online to trick or humiliate othersPlacing oneself at physical risk in order to take selfies or generate online contentCompulsive** use of social media including checking during the nightRefusing to remove a picture of someone else when askedCoercive behaviour toward others using digital technology (for example tracking others, accessing other people's accounts)Compulsive** use of pornographyWatching violent/extreme pornographyPressuring someone to send nudes/sext anlineAccessing extremist views read about onlineAccessing dark web*** to engage with services (for example buying drugs online, downloading extreme pornography)Accessing illegal contentShowing someone distressing videos they don't want to seeOnline dating with adultsForwarding nudes of other young people, including to friends. without consent
			including to friends, without consent

\*\*\*Deep web/dark web - the deep web is any website that is not indexed by search engines such as google. Accessing these sites is untraceable and they are often used to circumvent tracking that may be put on young people's devices. The deep web is not inherently illegal, however any young person using deep or dark web sites is incredibly vulnerable and therefore support should be offered even if they are accessing them for legitimate reasons (such as not wanting a parent to know they are exploring their gender or sexuality). The dark web refers to areas of the deep web where illegal activity takes place. Often young people will use these terms interchangeably.

# What to do when you have identified a behaviour

Most of the online behaviour young people engage in will fall into the 'Not Harmful' category. All of the online activities young people engage in can give you information about the young person's life, interests and concerns, which can in turn help you to engage with a young person, building a warm and understanding relationship. Expressing identity through online behaviour is a normal part of a young person's life. Professionals can sometimes feel intimidated by talk of apps and games that are unfamiliar and this can lead to being dismissive of activities that are important to a young person's identity, or overreacting to activities that are normal and low risk. This tool avoids naming specific apps or games\* and instead encourages professionals to use their existing skills and knowledge to respond to behaviours. When a 'Not Harmful' behaviour is identified, professionals can offer guidance and support to ensure healthy development continues. This could be through group or one-to-one sessions considering what risks young people might face in the future and how they think those risks could be managed (for example, it would be appropriate to discuss with 14-16 year olds the risks of online dating and to ask them how they might manage these risks).

Where behaviours are not age-appropriate, or represent harm to the young person or others, adults must intervene to help the young person and prevent further harm. We all have a duty to safeguard children and young people. You should refer to your organisation's safeguarding policy or report to the police or social services where appropriate. This tool aims to help you identify harmful behaviours and once identified you should use your safeguarding policy to proceed. We have listed some suggestions of how to respond to harmful or Potentially harmful behaviours below, but this does not replace or supersede your organisation's safeguarding procedures. When planning how to respond to a harmful or Potentially harmful behaviour, consider what support you might need to put in place to help the young person. For example, if a young person is being abusive to other people online, they may need to have an intervention focused on understanding the consequences of their behaviour, whereas if they have been sharing nude images of themselves they may need some selfesteem work, or their whole peer group may need some education on the risks and consequences of this behaviour.

Other ways to respond to harmful or Potentially harmful behaviours:

- Giving the child or young person information or signposting to reliable websites
- Giving families information and signposting or referring to services
- Modelling behaviour such as social media accounts set to private, time away from screens etc
- Helping the young person to identify safe emotionally available adults they can go to when they have questions
- Discussing precautions and ways of managing risk both on and offline
- Having consistency between home, family, school, community settings
- Having consistently enforced expectations of behaviour
- Extracting the young person from situations where they are experiencing or causing harm to others
- Limiting access to technology when behaviour becomes problematic (although cutting a young person off from technology completely may make them more vulnerable or secretive)

\*Although some police forces do release lists of apps and games of concern to professionals.

# **The Role of Education**

The Online Resilience tool will be an invaluable resource in the delivery of the Relationships Education, Relationships and Sex Education (RSE) and Health Education curricula, as it helps professionals to manage and moderate discussions and lesson delivery around normal, unusual, and abnormal online behaviours for a given age group. For the primary curriculum a lot of the behaviours listed in the tool will be addressed within the "Online Relationships" part of the curriculum. However, it will also support potential issues arising from areas such as "Being Safe" and "Respectful Relationships". For secondary education the tool primarily maps on to the "Online and Media " part of the curriculum but also supports issues raised in areas such as "Respectful Relationships", "Being Safe" and "Intimate and Sexual Relationships".

More information on the RSE curriculum for England can be found at: <u>https://www.gov.</u> <u>uk/government/publications/relationships-</u> <u>education-relationships-and-sex-education-</u> <u>rse-and-health-education</u>

# Online behaviour and the law

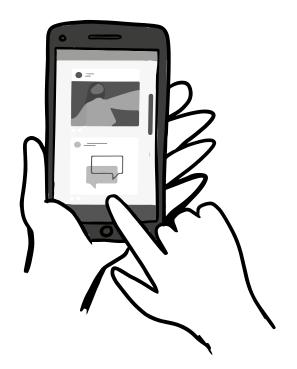
There is much discussion surrounding legal issues about online behaviour which are generally unhelpful and can lead to problematic outcomes for young people. This section provides clarification on a number of these issues.

## Minors accessing pornography

It is not illegal for a minor to access pornography (as long as the pornography is legal), and they should not be told they have broken the law if they disclose they have accessed it. However, neither of these legal issues mean that if someone under the age of 13 has a social media account they are breaking the law and they should not be told that they are.

# Accessing social media

There is a common belief that it is illegal for children to access social media under the age of 13. This is based upon US legislation that says it is illegal to advertise to a minor under the age of 13 without parental consent. More recently the Data Protection Act 2018 states that a minor under the age of 13 is not capable of consenting to their data being collected. However, neither of these legal issues mean if someone under the age of 13 has a social media account is breaking the law and they should not be told such. They are, however, breaching the terms and conditions of the social media site, as they have not been honest about their date of birth when they signed up. As such they are potentially at more risk because the social media site can claim no responsibility if they are subject to abuse. These are all reasons why we should be supporting minors who disclose upset arising from social media when they are under the age of 13.



# Sexting/sharing nudes

It is illegal for a minor to take an indecent image of themselves and send it to someone else. The law is defined in the 1978 Protection of Children Act, a piece of legislation developed to protect children from exploitation in the production of pornography. It never envisaged a time where the taker and sharer of the indecent image of a minor is also the subject of the image. While young people have been charged under this Act as a result of sharing nudes, in general it is the view of the Crown Prosecution Service that it is rarely in the public interest to prosecute a minor unless there is coercive, abusive or repetitive behaviour. Since 2016, police have been able to record such a crime as an "outcome 21". This means the crime is acknowledged but there is no public interest in pursuing a criminal case. We should not simply tell young people that sending nudes is illegal, as we risk re-victimising those who are being abused as a result of taking and sending an image. We should support them and help them resolve the issue, and involve law enforcement for their protection, not criminalisation.

## Upskirting

Upskirting (the taking of an image or video from beneath someone's skirt using a mobile device) has recently been made illegal in order to prevent people from engaging in these practices and to protect those who have been subject to this. While the recent Keeping Children Safe in Education update has raised the use of this legislation in schools to deter this behaviour among peers. However, this legislation is untested in the criminalisation of minors. While these behaviours are problematic among young peers, and warrants discussion and investigation, we have concerns that threatening minors with criminalisation as a result of these behaviour is disproportionate and counter-productive.

## **Online Gambling**

There is strict legislation around age limits for online gambling. The majority of online gambling has an age limit set at 18 and covers things like online betting systems, casinos, sports betting, etc. However, there are some forms of online gambling such as the national lottery and scratch cards (both of which can be carried out online) that have an age limit of 16. Other forms of "soft" gambling (such as loot boxes) are currently unregulated and are often in games played by younger children. While there is nothing inherently dangerous about loot boxes, professionals should be aware that there is a potentially compulsive element to purchasing them and people of all ages might spend excessive amounts of money on them.

# Glossary

#### **Child Sex Abuse Images**

Indecent images of children, either sexualised or engaged in sexual abuse. Often incorrectly referred to as "Child Pornography".

#### Coercion

Using threats or bribery to try to force someone to do something they would otherwise not want to do. Threats could be subtle, normalised within a relationship or group of friends, and with the coerced individual being told that other people would do/are doing it when that may not be the case (therefore differing from peer pressure). There will often be an element of fear, meaning that the coerced individual may concede in an attempt to get the coercion/contact to end.

#### **Critical thinking**

Being able to assess the validity of claims made through a variety of media. This could involve fact checking through websites such as Snopes, or using Google Scholar to see only peer-reviewed academic articles. It is important not to assume everything read online is false however as this can lead to apathy.

#### Cyberbullying

Online bullying, which is now frequently, and unfortunately, used to describe any kind of online abuse. Bullying requires some level of threat (either physical or emotional) and also requires persistent abuse. Its inaccurate use can cause us both to overreact to what we might refer to as brief online fallouts, and to devalue the impact of different types of abuse, for example harassment.

#### Dark Web

Specific parts of the deep web where illegal activity takes place. This may be the exchange of child sex abuse images, images of bestiality, and illegal forms of pornography. It may also include the planning of criminal activity such as drug dealing or terrorism.

#### Deep Web

Simply parts of the World Wide Web that are "hidden" from search engines and monitoring because all communication and access is encrypted and needs to be accessed using special software such as Tor browsers. While the dark web is used for criminal activities, the deep web is often used by those wishing to avoid government or state monitoring, particularly under totalitarian regimes.

#### Digital age of consent

The age in law where is has been decided a child is capable of giving consent to have their data collected online. As part of the GDPR, this age has been defined in the UK as 13. The digital age of consent is frequently used to argue why younger children should not be using online services and how it is illegal for them to do so. This is not the case, and the law has not been established for any safeguarding reasons. It is no coincidence that the Digital Age of Consent is the same as the age defined in the US's Children Online Privacy Protection Act (COPPA), the law that restricts social media companies based there to collect the data of children without parental consent.

#### **Extreme pornography**

Pornographic content defined as illegal in sections 63 to 67 of the Criminal Justice and Immigration Act 2008, for example bestiality, or pornography depicting physical harm. While possession of most pornography is not illegal, the possession of extreme pornography is and can lead to a custodial sentence.

#### Influencer

Someone on social media who makes recommendations about products or services in exchange for payment. Influencers are generally people with large online followings who generate considerable income. "Becoming an influencer" is attractive to some young people. However, in order to develop a large following an Influencer may need to expose themselves to risky online behaviours.

#### **Online grooming**

Making use of digital technology, such as social media or private messaging to trick, force or pressure a young person into engaging in sexual activity, for example sending an indecent image or live webcamming. While it is usual to expect grooming to take place between an adult and a child, grooming can take place at a peer to peer level too.

## Online Grooming re radicalisation and gangs

Young people may be groomed into gangs or radicalised thinking through the use of online grooming technique. This may go alongside faceto-face grooming, making it very difficult for the young person to have any thinking space or time away from those who are grooming them.

#### Online peer on peer abuse

Peer-on-peer abuse is any form of physical, sexual, emotional and financial abuse, and coercive control, exercised between children and within children's relationships (both intimate and nonintimate). Online peer-on-peer abuse is any form of peer-on- peer abuse with a digital element, for example, sexting, online abuse, coercion and exploitation, peer-on-peer grooming, threatening language delivered via online means, distribution of sexualised content and harassment.

#### **Online Radicalisation**

Someone being influenced to adopt an extreme or radical position on social or political issues using online means (messaging, persuasive media, etc.), for example to get someone to adopt a far-right or Islamist ideology.

#### Pornography

Is defined in the Digital Economy Act 2017 as any image, video, work classified as 'R18' - a special and legally restricted classification primarily for explicit works of consenting sex or strong fetish material involving adults.

#### **Revenge Porn**

The non-consensual sharing of an indecent image or video with others. This term is used for a situation involving a victim aged 18 or over. If the victim is a minor the act will be classed as the manufacture and distribution of indecent images of a minor.

#### Screentime

The term usually used to refer to how much time someone has spent online. While there is much concern regarding how much time young people spend online, there is insufficient evidence to show any clear impacts on mental health. However, recent advice\* by the Chief Medical Officer suggests a cautionary approach and not to dismiss screentime as a factor that has no impact on young people's mental health.

#### Sexting

The popular term for the exchange of indecent images using online or mobile devices (and sometimes used to describe sexualised messages). While the exchange of images such as this among young people is illegal, the legislation is complex and simple messages like "don't do it, it's illegal" will isolate those who might be being coerced or abused as a result of engaging in these activities. Young people are unlikely to apply the term 'sexting' to their behaviour, but may use terms such as 'nudes', 'dick pic', 'tit pic' etc.

#### Sexually Explicit Image/Video

An image or video which shows an individual, couple or group of people in a sexual context. This could be naked or fully clothed, undertaking or simulating a sexual act, or being filmed or photographed unknowingly.

#### Sharenting

The excessive, and often non-consensual, sharing of images and videos of their child(ren) online by parents without sufficient consideration of the impact of this on the child.

#### Trolling

Deliberately starting an argument or upsetting people online for one's own amusement. Saying something controversial online to upset others.

#### Webcamming

Using a webcam to live broadcast an interaction/ performance, often of a sexual nature, sometimes in exchange for money but also used in grooming.

\*https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/777026/UK\_CMO\_ commentary\_on\_screentime\_and\_social\_media\_map\_of\_reviews.pdf)

# **About Headstart**

This work was developed as part of the Digital work-stream of the HeadStart Kernow programme and was funded by The National Lottery Community Fund, the largest funder of community activity in the UK. HeadStart Kernow is a partnership programme led by Cornwall Council to develop resilience and mental well-being in young people in Cornwall.

Started in 2016, HeadStart is a five-year, £58.7 million National Lottery funded programme set up by The National Lottery Community Fund. HeadStart aims to explore and test new ways to improve the mental health and wellbeing of young people aged 10 to 16 and prevent serious mental health issues from developing. To do this, six local authority-led HeadStart partnerships are working with local young people, schools, families, charities, community and public services to design and try out new interventions that will make a difference to young people's mental health, wellbeing and resilience. The HeadStart partnerships are in the following locations in England: Blackpool; Cornwall; Hull; Kent; Newham; Wolverhampton.

### Acknowledgements and thanks

We would like to thank the children and young people of Cornwall who were involved in the development of this tool during the first three years of the HeadStart Kernow programme. Dialogue with young people took place in school settings:

- Large workshops drawing young people from different schools with facilitated discussion (attendance was around 60 students in each case)
- Discussion groups in specific schools with large student groups (30-40 in each group)
- Smaller discussion sessions in schools with 10-20 students in each group

In total we conducted 3 large workshops, 10 large discussion groups and 10 smaller discussion sessions. In total around 1000 young people were spoken to in this phase of the work.

## **About the authors**

Professor Andy Phippen is Professor of IT Ethics and Digital Rights at University of Bournemouth. Louisa Street is an education specialist and youth worker based in Cornwall who has experience working with young people around issues such as mental health, sexual health, drugs and alcohol. The Professionals Online Safety Helpline (POSH) at South West Grid for Learning is co-funded by the European Commission and was set up in 2011 to help all members of the community working with or for children in the UK, with any online safety issues they, or children and young people in their care, may face.

The authors would like to acknowledge the contribution of Ben Bolton and Dr Sarah Canavan-King to this work, whose passion, enthusiasm, and initial discussions with young people and the children's workforce laid the foundation upon which it was built.

#### www.headstartkernow.org.uk

#### 🗩 www.startnowcornwall.org.uk

log hskyouth (f) hskyouth (f) hskyouth



This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <u>http://creativecommons.org/licenses/by-nc-nd/4.0/</u> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.



© HeadStart Kernow 2020

HeadStart Kernow is supported by funding from The National Lottery Community Fund and is delivered by Cornwall Council. The Online Resilience Tool has been produced with support from Bournemouth University and SWGfL