UK Council for
Internet Safety

Digital Resilience Framework

A framework and tool for organisations, communities and groups to help people build resilience in their digital life.

1. Introduction

Today, people are growing up in an increasingly digital world. Digital technologies are present in most areas of life. People socialise, explore, create and work in digital environments. Organisations, groups and communities are increasingly connected as technology becomes more pervasive. People will encounter risks during these online experiences and it is neither possible nor desirable to shield them entirely from risk. Learning how to recognise and manage risk, learn from difficult experiences, recover and stay well, is a vital part of individual development and agency.

Resilience can be defined as 'a process to harness resources to sustain wellbeing', and digital resilience as the application of this concept to technology, the internet and the digital age. Digital resilience helps individuals recognise and manage the risks they come across when they socialise, explore or work online. It is achieved primarily through experience, rather than learning and it is fostered by opportunities to confide in trusted others and later reflect upon online challenges.

What is this document?

This UKCIS Digital Resilience Framework is a practical, easy-to-use document designed to help organisations consider and support digital resilience for both individuals and groups. It includes an introduction to digital resilience and a checklist for different content, services, environment and policies. The overall aim is to provide a shared focus for decision making, placing digital resilience at the centre of considerations for organisations, communities and groups.

This Framework is a product of the UKCIS Digital Resilience Working Group Policy Paper, which provides a more detailed explanation of digital resilience, including how the definition was developed and a more extensive checklist with consideration for various internal and external factors in different settings.

Who is this document for?

It is for use by all of the people and organisations involved in supporting, managing and creating people's interaction with connected technologies. The implementation of the Framework should be seen as additional support to existing statutory obligations. In particular, close consideration should be given to the role of the Framework in relation to safeguarding for vulnerable children or adults in which additional safety and protection may be a requirement.

It looks at four key domains that will impact on people's experiences in an increasingly connected digital society:

Environment
Including any access point to the internet. This includes a wide range of private and public spaces, from residential settings through to education establishments, public institutions (e.g. libraries) and informal settings (e.g. community centres).

Content
Including entertainment and educational content, terms of service and any messaging about the use of digital.

Service
Including devices, platforms, apps, games and websites.

Policy
Including local, national and institutional policies.

No domain will exist in isolation and people's experience online will occur across multiple contexts.

Two steps to using the Digital Resilience Framework

1	Understanding Digital Resilience
2	Self Assessment

Feedback and Development

The Digital Resilience Framework is continually evolving and we would welcome your feedback. We would particularly value any thoughts or comments on the impact of using the Framework to build resilience in your sector.

About us

The Digital Resilience Framework was developed by members of the UK Council for Internet Safety (UKCIS) Digital Resilience Working Group. Bringing together leading organisations in online safety and harms - including the BBC, BBFC, CEO, Childnet, The Diana Award, Facebook, Google, Trust and Safety Group, Internet Matters, Marie Collins Foundation, The Mix, NSPCC, Ofcom, Parent Zone, Carnegie Trust and PSHE Association - helped develop a collective Framework which effectively focuses on building and promoting the need for greater digital resilience.

UKCIS is a collaborative forum between the government, tech community and the third sector. Working together with the Department for Digital, Culture, Media & Sport, the Department for Education and the Home Office and across the breadth of online harms helps UKCIS to ensure the UK is the safest place in the world to be online.

For more information on UKCIS or the range of online harms go to https://www.gov.uk/government/organisations/uk-council-for-internet-safety

2. Definitions

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.

Features associated with resilience

- Planning tendency (propensity to plan).
- A style of self-reflection as to what worked, and what didn't work.
- A sense of agency or determination to deal with challenge.
- Self-confidence in being able to deal with challenges successfully.

Understand

An individual understands when they are at risk online and can make informed decisions about the digital space they are in

Know

An individual knows what to do to seek help from a range of appropriate sources

Learn

An individual learns from their experiences and is able to adapt their future choices, where possible

Recover

An individual can recover when things go wrong online by receiving the appropriate level of support to aid recovery

How is digital resilience established?

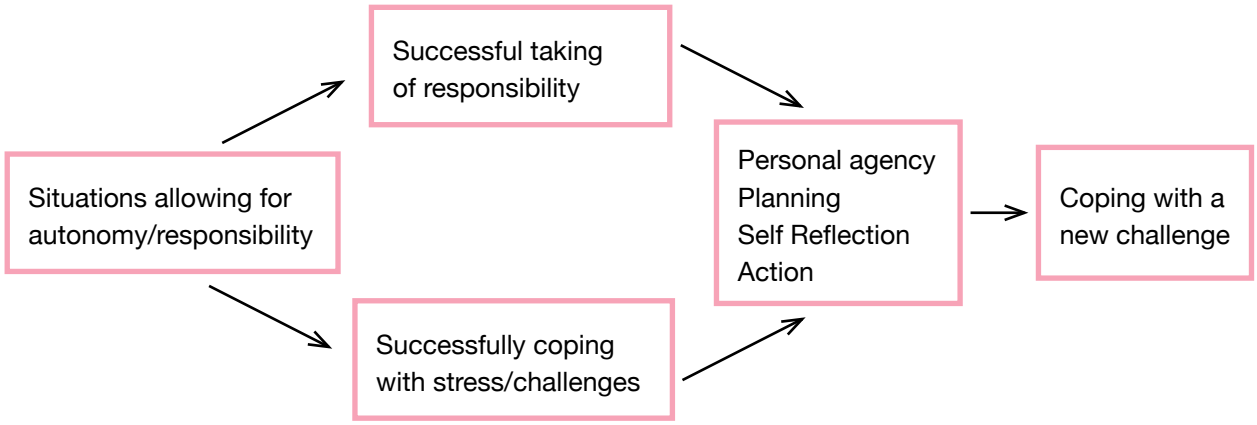
It is primarily built through experience rather than learnt, fostered by opportunities to confide in trusted others and later reflect upon online challenges. Growing self-control and an ability to recognise what is harmful, and respond appropriately, are key aspects.

How is it developed?

It is developed through online activities in safe managed environments which enable knowledge, skills and confidence for the individual to develop and cope with the negative consequences of online stress. This goes hand in hand with appropriate support and guidance the individual may want or need. Having support to recover and re-engage with digital opportunities are equally important.

How can you support it?

Thinking about the most appropriate ways to support digital resilience involves balancing internal and external factors in order to create environments which foster resilience.



3.
Self Assessment

Gather information thinking about a person's age and any additional internal or external factors. Consider relevant technology options, legal requirements and local resources. For a more detailed explanation of how to use the Self Assessment and which key factors should be considered, please refer to the Digital Resilience Working Group Policy Paper.

- Complete the Self Assessment
- Use the review checklist

Environment
Public and private providers of access to the internet

Content
Those who create, provide or deliver content for learning resources, support or events related to internet use

Service
Those who design, develop or manage digital services

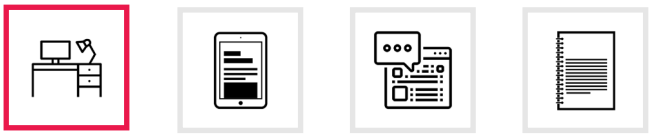
Policy
Those who create, implement or review policies that may impact on people's access, use and understanding of the internet and digital services

Additional Factors

There are a variety of internal factors and external factors which should be considered when using the Framework and assessing whether your organisation is building resilience. This non-exhaustive list outlines a few key considerations which should be accounted for in addition to mandatory safeguarding procedures:

Internal Factors
- Vulnerabilities
- Isolation
- Longing for a sense of belonging
- Searching for an identity
- Experiencing mental and cognitive health issues

External Factors
- Targeting of vulnerable users
- Age considerations



Environment

Understand
Are people encouraged to understand and manage different types of risk in an age-appropriate way when they are online?

Know
Are people adequately supported to respond to risk, in particular to risks posed by online harms?

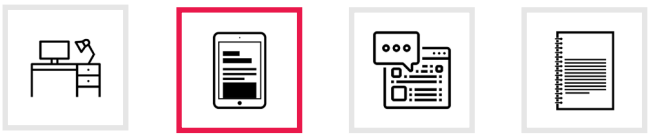
Learn
Does your environment provide opportunities for people to reflect, re-engage and practise skills after online experiences?

Recover
How are people encouraged to access appropriate recovery services?

For more details please refer to
UKCIS Digital Resilience Working Group Policy Paper

Things to consider
Think about the age appropriateness of your environment and how it helps people engage and find support services in an understandable user-friendly way.

Internal/External Factors
Think about what other factors may need to be considered that might be internal or external.



Content

Understand
Do your resources help people recognise and differentiate between different types of risks?

Know
Do your resources offer advice on actions to take once a risk has been identified? Are your signposted resources trustworthy?

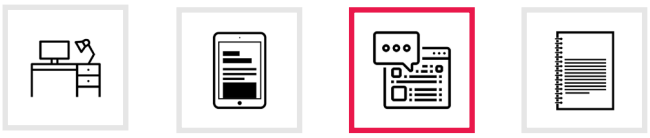
Learn
Do your resources help people change their settings and online behaviours to prevent online harms. Does this encourage pro-social behaviour?

Recover
Do your resources encourage users to seek further support from other suitable networks should the user have suffered harm?

For more details please refer to
UKCIS Digital Resilience Working Group Policy Paper

Things to consider
Think about the design of your content and any signposted resources, and whether they support people to confidently manage risk.

Internal/External Factors
Think about what other factors may need to be considered that might be internal or external.



Services

Understand
Does your service enable users to assess risk and manage their experience using tools and settings, in an age-appropriate way?

Know
Does your service allow users to report in a user-friendly, age-appropriate way?

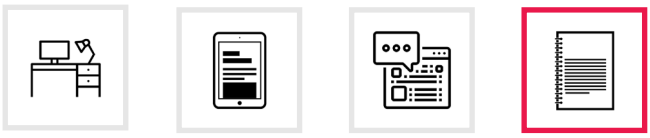
Learn
Does your service support users to understand reporting outcomes and adapt their behaviour to lower the risk of future harms?

Recover
Does your service provide appropriate support to users who may be at immediate risk of serious harm, and what further support is offered following a harmful online experience?

For more details please refer to
UKCIS Digital Resilience Working Group Policy Paper

Things to consider
Think about your reporting procedures and how they support a recovery stage following a harmful incident.

Internal/External Factors
Think about what other factors may need to be considered that might be internal or external.



Policy

Understand
Do your policies help a widespread understanding of online risks and harm to promote positive use of the internet whilst minimising inappropriate digital measures, in an age-appropriate way?

Know
Do your policies promote measures that enable people to seek and receive help, in particular, by encouraging an adequate support ecosystem able to deal with online harms?

Learn
Do your policies support opportunities to learn from negative online experiences?

Recover
Are your policies supporting the creation and sustainability of support services for users who suffer severe harms as a result of online harms?

For more details please refer to
UKCIS Digital Resilience Working Group Policy Paper

Things to consider
Think about how your policies support resources and services which help people have a positive experience online.

Internal/External Factors
Think about what other factors may need to be considered that might be internal or external.

Self Assessment Checklist

Having considered the above, please complete the following checklist to assess how well your domain or domains of influence promote each aspect of digital resilience. Please tick one box.

	Poorly	Moderately	Well
People are given appropriate access to online services.	☐	☐	☐
People are encouraged to recognise risk.	☐	☐	☐
People are encouraged to differentiate between varying types of risk.	☐	☐	☐
People are encouraged to report harms.	☐	☐	☐
People are encouraged to use varying reporting mechanisms.	☐	☐	☐
People are encouraged and supported to adapt behaviours where possible to reduce future harms.	☐	☐	☐
People are encouraged to seek recovery services should a severe harm be suffered. People are provided opportunities, and encouraged to inform/review/co-create the system to reduce risk or improve opportunities for others.	☐	☐	☐

List of Members

Having used the checklist, please find a list of member organisations who provide online safety resources and guidance. Under the new UKCIS online harms mandate, we expect the list of signposted resources to increase as new members and sector organisations join the group. Current members include:

- BBC
- BBFC
- NCA - CEOP
- Childnet
- Department for Digital, Culture, Media & Sport
- Department for Education
- Department of Health
- Good Thinking: the London Digital Mental Wellbeing Service
- Google
- Home Office
- Facebook
- Internet Matters
- Marie Collins Foundation
- NSPCC
- Ofcom
- Parent Zone
- PSHE Association
- The Diana Awards
- The Mix
- Trust and Safety Group
- Twitter
- Vodafone
- Virgin Media
- UKIE


BBC


bbfc
View what's
right for you


CEOP
A National
Crime Agency
command


Childnet
International


Department for
Digital, Culture,
Media & Sport


Department
of Health &
Social Care


Department
for Education


Home Office


Google


internet
matters.org


MCF
The
Marie Collins
Foundation


NSPCC


Ofcom
making communications work
for everyone


Digital Resilience Framework Architects
parentzone


PSHE
Association


THE
DIANA
AWARD


THE MIX


NHS


Trust + Safety Group


vodafone


Virgin
media


ukie
THE ASSOCIATION FOR UK INTERACTIVE ENTERTAINMENT


UK Council for
Internet Safety