UK Council for
Internet Safety

Digital Resilience Working Group Policy Paper

1. Introduction

Background and Context

UKCIS

The UK Council for Internet Safety is designed to provide internet safety for all users, building on the pioneering work of UKCCIS which had specific objectives reflecting children and young people’s special needs for care and protection. New priority areas under UKCIS include online harms, such as cyberbullying and sexual exploitation; radicalisation and extremism; violence against women and girls; hate crime and hate speech and forms of discrimination against groups protected under the Equality Act, for example on the basis of disability or race.

Digital Resilience Working Group

Under the UKCIS mandate, the Digital Resilience Working Group works with the Home Office, Department for Digital, Culture, Media & Sport, Department for Education and the Department of Health in these designated areas of focus, to ensure it delivers on its aims and objectives. The group also shares and promotes digital resilience best practice with the UKCIS Executive Board, other UKCIS working groups, the wider stakeholder community, as well as the public. It will continue to do so as and when the digital resilience Self Assessment section of this paper is used by organisations. For a list of all members of the group please see page 17.

Digital Resilience Working Group Policy Paper

Developed by the members of the Digital Resilience Working Group, this policy paper defines digital resilience and is designed to provide a simple process for organisations to assess whether different types of environments, content, online services and policies support, or hinder, digital resilience.

Digital Resilience Framework

The Digital Resilience Framework is a condensed version of this policy paper, which serves a similar purpose as a practical, easy-to-use document to help organisations consider and support digital resilience for both individuals and groups. There is no set way to use these documents and the Digital Resilience Framework and Policy Paper can be used together or independently.

Publication of Digital Resilience Documents

All documents listed above are published by the group and are available under open government licence.

Purpose of this paper

The decisions of a wide range of people affect how people access the internet and the type of experience they have online. For a young person, this could include people close to them, such as parents, carers and teachers, as well as those at a distance, such as government policy makers and online service providers, which may have an impact on all users.

These decisions will affect the ways in which all people access the internet, the information they receive and the design of the services they use. Users' choices range from the individual – what filters to apply in a home or other residential settings – to the international – what privacy settings to provide on a platform. Often these decisions will be based on different and sometimes conflicting priorities, from concerns about safety to commercial considerations. This patchwork of choices creates the conditions in which people experience the online world.

This paper provides a shared focus for decision making, placing digital resilience at the centre of considerations for organisations, communities and groups. It aims to shape policy, education, parenting and service design whilst complementing other resources and guidance, which should be read in conjunction. Examples of compatible documents might include:

- The UKCIS education framework 'Education for A Connected World';
- The Home Office Prevent programme;
- The social media guide for providers of social media and interactive services;
- The Department for Education Keeping children safe in education: for schools and colleges statutory guidance.

This paper should be used,

- to foster a shared understanding of digital resilience.
- to encourage best practice and provide 'real life' examples of positive digital resilience initiatives.
- as a checklist and practical tool to aid decision making.
- as a reflection tool to assess the likely impact of policy or service design.

It can be used at any stage in these processes from planning to implementation; monitoring to evaluation.

Scope of this paper

This paper is for use by all of the people and organisations involved in supporting, managing and creating people's interaction with connected technologies.

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.

Implementation of this paper

This paper is currently split into two sections, with the aim of including best practice examples, additional resources and case studies, as and when the paper develops;

- Understanding Digital Resilience
- Self Assessment

The implementation of this paper should be seen as additional support to existing statutory obligations. In particular, close consideration should be given to the role of this paper in relation to safeguarding for vulnerable children or adults in which additional safety and protection may be a requirement.

The Digital Resilience Framework is a condensed version of this paper which can be used in a similar way.

2.

Understanding Digital Resilience

What is Digital Resilience?

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.

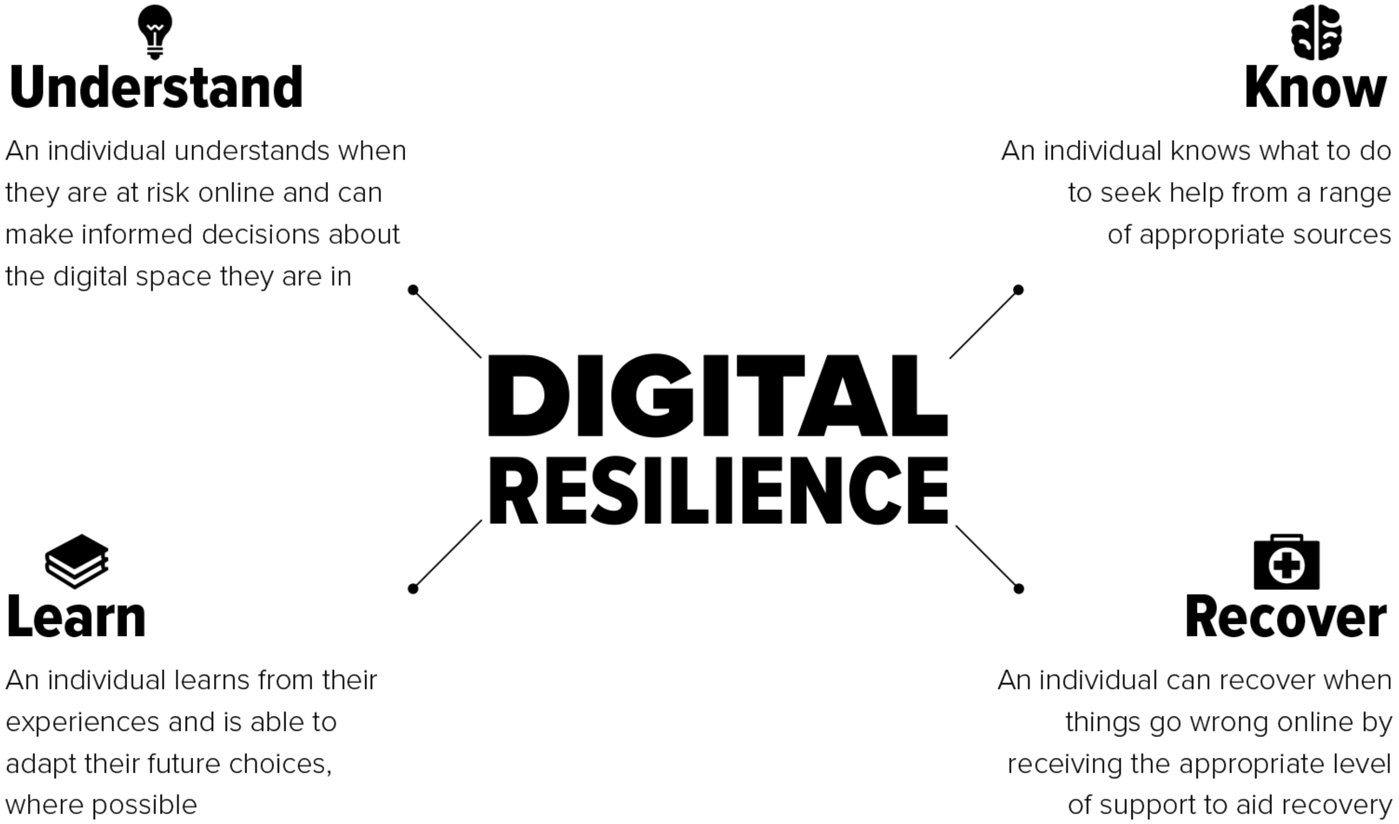
What is it?
Digital resilience is a dynamic personality asset that grows from digital activation i.e. through engaging with appropriate opportunities and challenges online, rather than through avoidance and safety behaviours.

How is it 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 is equally important.

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.



DIGITAL RESILIENCE

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

Supporting resilience

Digital resilience is not a fixed state. It is a dynamic personality asset, meaning people can be more or less resilient depending on their environment, experiences and circumstances at any given time.

Families, carers, educators, policy makers, frontline service workers and industry all have a role to play in making sure that they are contributing to an ecosystem that supports resilience and does not undermine it.

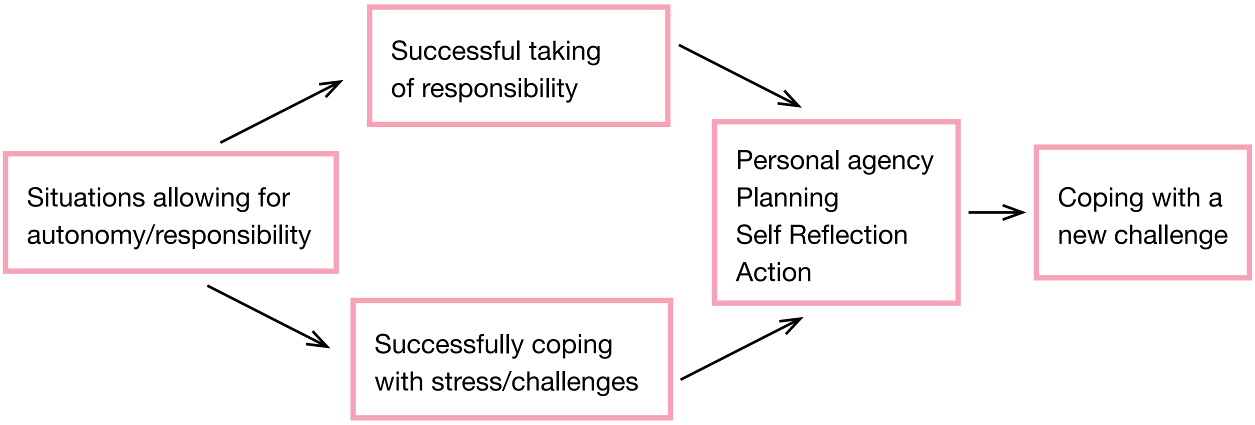
When thinking about supporting resilience it is important to remember that online, just as offline, there are complex social interactions with internal and external factors, as well as assets and deficits that impact users.

Internal factors might be vulnerabilities, such as feeling isolated, longing for a sense of belonging, searching for an identity or experiencing mental and cognitive health issues. This could lead to a person - knowingly or unknowingly - seeking something that could be harmful to them.

External factors, like the actions of those who deliberately target vulnerable people online, also need to be considered.

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

Resilience pathway


Successful taking of responsibility
Situations allowing for autonomy/responsibility
Personal agency
Planning
Self Reflection
Action
Coping with a new challenge
Successfully coping with stress/challenges

3.
Self Assessment

3.1. Environment

Guidance for providers of access 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).

Understand when you are at risk online	Self Assessment
Are people able to explore online in managed, age-appropriate ways?	Describe steps taken to ensure people have age-appropriate access. This could include the use of filters and parental controls, guided and curated access (e.g. digital reading lists, white lists etc). Consider how your environment balances the need for people to have access to explore with the requirement for safety.
Are people encouraged to recognise risk?	Describe the ways in which people are encouraged to recognise risk. Examples might include formal lessons, one to one support, content warnings and ratings, etc. Consider how your environment promotes the need for individuals to identify and manage risk whilst simultaneously protecting people from harm. Also, give consideration to how risks are recognised and supported in relation to the individual's context: i.e. additional vulnerabilities and wider circumstances.
Are people able to understand and differentiate between functionality risks (e.g. anonymity, live streaming, fraud) and behavioural risks?	Describe the ways in which people are encouraged to understand functional and behavioural risks in your setting. Consider whether you appropriately communicate risks to people who have a range of access and support requirements.

3.1. Environment (continued)

Know what to do to seek help online	Self Assessment
Are users encouraged to respond to risk accordingly?	Describe the ways in which people are encouraged to respond to risk in your setting. Examples might include having a designated person to report to, lessons in how to report, peer to peer support groups etc. Consider whether you provide available, accessible and appropriate help for the people most at risk. Are people able and encouraged to inform, review and co-create the service, setting, content or policy themselves?
Are appropriate responses in place to deal with reports of online harms?	Describe how you deal with reports of online harms from people. Consider whether the context of peoples wider circumstance and digital experience are factored in to your online harms response.
Learn from experience	**Self Assessment**
Are people given opportunities to reflect on online experiences?	Describe how you encourage people to reflect on online experiences. Consider how your environment encourages transparency and user awareness, whilst providing reassurance and additional support to aid recovery.
Are people able to re-engage and practise skills?	Describe how you encourage users to practise new skills and to re-engage with online services following challenges. Consider whether the opportunities provided for people to re-engage are tiered to support people with different requirements and experiences.
Recover when things go wrong	**Self Assessment**
Are users encouraged to access appropriate recovery services?	Describe how you support recovery. Examples might include school counselling, signposting to NHS support, peer to peer support networks etc. Consider whether you provide effective access to additional support, perhaps by effective signposting to specific services.
Does everyone know how to respond to reports of online harms?	Describe how you respond to reports of online harms. Examples might include statutory training, safeguarding policies, student support structure, family agreements. Consider whether you have the knowledge or links to assist people who may have additional support requirements.

3.2. Content

Guidance for those who create, provide or deliver content for learning resources, support or events related to internet use. This could include formal lessons, non-formal resources or physical events. Whilst these are likely to be primarily designed for direct users, information for development and training of professionals may also be included.

Understand when you are at risk online	**Self Assessment**
Do the resources help people to recognise risk?	Describe how the content helps users to recognise and identify online risks. Examples of risk may include suspected phishing attacks or extremist content, or a web page that isn't secure. Consider whether your resources address how potential risks may be informed by other similar people's experiences.

Know what to do to seek help online	**Self Assessment**
Do the resources offer advice on what action to take once a risk has been identified?	Describe how the resources help users to manage risk. Examples might include practical tips like turning off cameras or chat in gaming to address the risk of exposure to bad language. Consider whether your resources address how users might report to the platform, seek further help and modify their behaviour.
Do the resources signpost people to trusted support networks?	Describe how the resources direct users to available support. Examples might include parents, carers, helplines, police and health professionals. Consider whether your resources address additional support networks, such as peer support groups, family support and the role of designated safeguarding leads.
Do the resources help people to understand functionality risks and behavioural risks?	Describe how the resources help users identify and differentiate between different types of risk. Examples of behavioural risk might include accessing explicit content, examples of functionality risk might include profile settings automatically sharing personal information. Consider whether your resources address how the behaviours of your users may impact potential risks.

3.2. Content (continued)

Learn from experience	Self Assessment
Do the resources help people change their settings and online behaviours to prevent further harms?	Is reasonable consideration given to individuals' ability to confidently utilise tools or adapt choices? Examples might include; tutorials in tools and settings, reducing time spent online, changing online diet. Consider whether your resources address the need for further support and how additional vulnerabilities may make this more difficult for some people.
Do the resources encourage self reflection?	Describe how the resources encourage users to reflect on their own experiences. Examples might include interactive exercises, discussion topics or self-monitoring tools. Consider whether your resources encourage the ability of individuals to positively reflect and, if not, what additional support may be required for this.
Do the resources encourage pro-social online behaviour?	Describe how the resources encourage positive online behaviours on behalf of the wider digital community. Examples might include empowering self-moderated online communities, encouraging peer reporting etc. Consider whether your promoted types of pro-social behaviour are reviewed and reflected by the people actually using the resources.

Recover when things go wrong	Self Assessment
Do the resources encourage users to seek further support from other suitable networks should the user have suffered harm?	Describe how the resources signpost or empower users to use trusted services and support networks. Examples might include NHS support, family support and law enforcement. Consider whether your resources promote networks which are relevant and informed by the people actually using the resources.

3.3. Services

Guidance for those who design, develop or manage digital services. This could include websites, games or apps, emerging technologies such as internet connected devices or virtual assistants.

Understand when you are at risk online	**Self Assessment**
Does the information provided on your service enable users to assess risk?	Describe measures taken to ensure information is available to all users to help them assess risk. Examples might include translations into local languages; accessible language and design for all ages and abilities. Consider whether your provisions are clear and can be understood by your range of users.
Does the service allow users to manage their experience using tools and settings?	Describe the manual and automatic options available to users to manage their digital experience. Examples might include filtering by subject; blocking specific users or pages; and managing privacy settings etc. Consider whether the options available to users are understandable to the different types of users.
Does the service impose age restrictions to ensure users are the appropriate age?	Describe the measures taken to ensure the service is not accessed by users of an inappropriate age. Examples might include terms and conditions and age verification. Consider whether your service restricts users of an inappropriate age and how this makes people aware of consent.

3.3. Services (continued)

Know what to do to seek help online	Self Assessment
Does the service offer a reliable reporting mechanism?	Describe how the reporting system has been designed to improve the service and meet users' concerns. Examples may include use of technology/moderators in dealing with reports, as well as speed of outcomes. Consider whether people are appropriately informed of the outcomes of reports, how they are provided with relevant context and whether there are any alternative support and reporting options provided.
Is the reporting system designed to be user friendly?	Describe how the reporting system has been designed to benefit the user. Examples might include anonymised reporting process; good communication throughout the reporting process; communication of reasons for report outcome with user, easy to navigate reporting options. Consider whether your service addresses different circumstances and experiences of users which may impact how individuals benefit from reporting systems.

Learn from experience	Self Assessment
Does the reporting mechanism ensure users understand report outcomes?	Describe how the reporting system informs users on the outcome of a report and the reasons for the outcome. Examples might include feedback on unsuccessful reports; details of the report process, service level reports on user reporting levels and outcomes. Consider the clarity of your reporting service and whether it respects individual sensitivities of different users when informing them about the reasons for the outcome of a report.
Does the service help users adapt behaviours to lower the risk of future harms?	Describe how the service helps users adapt their behaviours. Examples might include suggested settings alterations, promotion of positive content etc. Consider whether your service addresses the individual's ability to confidently utilise tools or adapt to choices, including what additional support may be required for this and vulnerabilities which may make this more difficult for some people.

3.3. Services (continued)

Recover when things go wrong	Self Assessment
Does the service encourage users to seek further support from other appropriate networks should a user suffer harm?	Describe how the service helps users find support networks in the event of a severe harm. Examples might include signposting to counselling services, promoting reliable support services, in-platform experts etc. Consider whether the networks that are promoted are informed and reviewed by people actually using the service.
Does the service have appropriate intervention measures for users suspected to be at urgent risk of harm?	Describe how the service has considered the need to make emergency referrals. Examples might include automated processes, human moderation etc. Consider whether your service addresses the different experiences and circumstances of users and how this might impact the appropriateness of intervention measures.

3.4. Policy

Guidance for those who create, implement or review policies that may impact on people's access, use and understanding of the internet and digital services. This is likely to include local authorities and government departments but may also include employers. Consideration should also be given to how wide reaching policy decisions affect the ability of other spheres of influence which foster resilience.

Understand when you are at risk online	**Self Assessment**
Do policies promote universal, age appropriate access to online services?	Describe how policies promote access to age-appropriate online services. Examples might include network speed; infrastructure. Consider whether your policies address the different needs, experiences and circumstances of users and how this might impact access to online services.
Do policies promote widespread understanding of online risks and harm?	Describe how policies promote understanding of online risks and harm. Examples might include educational programmes; family support, public information campaigns etc. Consider whether your policies can be understood by those who are at potential risk of experiencing online harm.
Do policies promote positive use of the internet and minimise inappropriate digital avoidance measures?	Describe how policies will contribute to fostering the positive use of the internet whilst avoiding measures that might result in users not engaging with digital technologies. Consider whether your policies allow for positive use of online services and how this use may be different for different users.

3.4. Policy (continued)

Know what to do to seek help online	Self Assessment
Do policies promote measures that enable people to seek and receive help?	Describe how policies support the provision of, and access to, help. Examples might include transparency reporting; minimum safety by design standards and public health campaigns. Consider whether your policies address the different types of support that people might need to seek and receive help.
Do policies encourage an adequate support ecosystem able to deal with online harms?	Describe how policies encourage a successful support system responsive to the needs of people who have experienced harm online. Examples might include support at local and national levels; family support; environment specific support networks. Consider whether your policies address both the online and offline impact of harms and how this may impact people in different ways.

Learn from experience	Self Assessment
Do policies support opportunities to learn from negative online experiences?	Describe how policies support wider education about online harms. Consider whether your policies provide additional support to promote transparency and explain why negative online experiences may occur, whilst addressing how individual circumstances may impact this.

Recover when things go wrong	Self Assessment
Are policies supporting the creation and sustainability of support services for users who suffer severe harms as a result of online incidents?	Describe how policies support recovery of users who have suffered severe harms. Examples may include NHS services. Consider whether your policies respond to the impact that severe harms may have on different users and whether adequate support services are in place.

3.5. 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

f

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