the space

Online abuse in the cultural sector: how to prepare and respond

A toolkit

Introduction



Fiona Morris

CHIEF EXECUTIVE & CREATIVE DIRECTOR, THE SPACE

The Space has been helping artists and cultural organisations to develop digital projects and skills since 2012. During this time, the opportunities to create and promote content and engage with audiences online have exploded. But so too has the pernicious behaviour of online abuse and harassment towards artists and other creatives. Alarming for organisations and deeply disturbing for individuals, as the UK's digital arts agency The Space felt that we had to act.

In 2019, we conducted a small survey of UK-based artists and cultural organisations on the theme of Artistic Freedom of Expression and the Internet in collaboration with **Index on Censorship**. The results were saddening but not surprising. Our communication with those working in the culture sector today, as well as reports from the Victims' Commissioner, sadly gives us no reason to believe the situation has improved in the intervening years.

Our research revealed that almost half (42%) of respondents had experienced virulent criticism or attacks online, including online abuse, trolling and personal attacks. When this figure was broken down, more women than men reported attacks online. Only 17% felt they knew how to deal with it.

Furthermore, 69% of respondents thought that fear of censure and online attack impacted upon freedom of expression and fear of this kind of abuse was the main factor impacting artistic freedom online. A more detailed breakdown of the survey results can be found on **pages 7-8.**

The Space wants to help the sector plan for and respond to this malevolent and harmful issue. We are not trying to curb fair criticism or free speech in any way – but instead focus on where 'criticism' bleeds into abuse and harassment and leaves victims in its wake.

We hope this toolkit offers some of this much-needed guidance. It's not intended to be either exhaustive or definitive, and for those individuals and organisations caught up in a storm of online abuse, we recommend that you consider seeking professional help – whether that's for legal, communications or emotional support. There is a list of helpful resources at the end of this guide.

In this toolkit, you will find: the results of The Space's survey; personal perspectives on online abuse and its impact; questions that teams at cultural and heritage organisations can ask themselves as a starting point for planning how they want to handle an online attack; a guide to privacy settings and why they are important; a checklist of what you can do if you find yourself victim to an attack; details about The Space's own approach to preparing for and handling abuse online and the services we offer to other organisations; and, contact details for other resources and organisations that can support you.

Digital-born content and online audience engagement are exciting ways to use technology and new ways of making art and offer exciting opportunities to connect with our audiences. Let's not lose sight of that as we face the darker corners and voices of the web together as a sector.

Foreword



Yumna Al-Arashi
ARTIST

Artists today face a largely unacknowledged and complicated vulnerability: harassment and abuse online. Although the democracy of digital spaces has allowed us to expand our reach, and has even fostered new techniques of creating art, it has also left us in a wildly vulnerable position for attacks, often from anonymous sources.

This complicated issue has left governments and organisations struggling to find solutions – most online harassment stems from the dark roots of our society's problems. Artists often feel they have no resources to combat the problem, and find themselves self-censoring as the first mode of defence.

Rather than trying to find an end-all approach to online harassment, we wanted to create an accessible resource for artists to support them when they need it most. This is where this toolkit began.

As an artist who has experienced online harassment and self-censorship multiple times over the years, I often had to find solutions and community on my own, feeling there was little or no resource to guide me.

Resources which already existed often felt sterile and confusing. As a financially-restricted artist, the looming fear that legal resources would need to come into play deterred me and my peers from seeking legal help. And even then, how could the law help us when there are often no laws protecting us from such a new and daunting form of harassment? Attacks are so often aimed at women, people of colour, and many other marginalised groups. So how, then, could we seek safety online if we can't find it in our physical worlds?

The harassment is often relentless and has a major emotional impact. It can cause us to shut down, remove ourselves from the problem entirely: self-censoring as a mode of protection. Our online spaces are no longer safe spaces for expression, therefore limiting the chance of a wide breadth of equally representative voices. The internet, in effect, has become a space of privilege which often neglects to take care of those most vulnerable to harassment.

So how do we help artists in these situations? How do we create, design, and engage spaces where artists feel empowered and not at risk? How can we provide resources which allow a larger conversation to take place around censorship, online harassment and privilege online?

This toolkit, and the broader programme of work The Space is doing around this issue, is a first step in trying to address some of these questions, and to push the topic of online abuse up the sector's agenda.

Contents



If you are reading this and currently under attack online, please click here to go to page 33 for guidance on what to do now.

Part 1: What's the problem? 5
The Space's research into online abuse in the arts

How does the arts and heritage sector experience online abuse? 6

How big is the problem? 7

Part 2: What do we mean when we talk about online abuse? 9
Terminology and definitions

Part 3: What does online abuse feel like? Is it a freedom of speech issue? 12
Personal perspectives

An artist's experience of being the target of abuse online – Yumna Al-Arashi 13

An organisation's experience of being at the centre of a media storm – Manchester Art Gallery curator Clare Gannaway speaks to Natalie Woolman about #nymphgate 15

What is it like being an organisation targeted by abuse online? – Rowan Kerek Robertson, Social Media and Digital Content Consultant & former Head of Social Media, BBC Television 18

Part 4: What can we do about it before it happens? 22
How to do an online abuse audit: A guide for organisations

Part 5: What can we advise individual artists and team members? 28
Privacy settings and what to do when you are subject to an attack online

Why privacy check-ups are vital and what to think about – Rowan Kerek Robertson, Social Media and Digital Content Consultant & former Head of Social Media, BBC Television 29

Privacy Check-up – What to consider… 30

Are you currently being attacked: Checklist to get through the Here And Now 33

Part 6: What is The Space's approach to tackling the issue of online abuse? 35

Part 7: Resources 37

Resources and helpful links 38

Appendix 1: When is online abuse a crime? 40

The Space offers a range of support to help arts and heritage organisations plan for and respond to online abuse. These services include risk assessments, consultancy for organisations looking to draw up policies and protocols to deal with online abuse and bespoke training for managers and teams. To find out more, please email **contactus@thespace.org**

Part 1

What's the problem?

The Space's research into online abuse in the arts

How does the arts and heritage sector experience online abuse?

Online abuse can affect people working in the cultural sector in different ways. In this toolkit, we include perspectives and advice both for organisations looking to plan for an online abuse incident and for individuals dealing with the issue, whether they are employees, freelancers or individual practitioners.

Some sections are focused specifically on either the organisational or individual experience: **Part 4** is designed for organisations looking to prepare for an incident of abuse online before it happens and **Part 5** is geared towards individuals, and includes guidance around online privacy settings and a checklist for what you can do if you are under attack now.

Of course, the individual and organisational experience are often fundamentally linked – the individual under attack might be a team member or a commissioned freelancer, and any organisation is made up of individuals. Therefore, we recommend that the sections above are not read in isolation, but holistically alongside the rest of the toolkit.

There are a number of ways online abuse can be encountered within the cultural and heritage sector. These include:

- **An organisation is subject to online abuse**
- **An employee is subject to online abuse related to their work for the organisation**
- **An employee is subject to online abuse for external reasons but targeting both work and personal accounts**
- **A commissioned artist is subject to online abuse related to work commissioned by the organisation**
- **A regularly commissioned artist is subject to online abuse for an independently-commissioned piece of work**
- **The organisation is drawn into a more generally contentious position online**

How big is the problem?

In 2022 the serious harm that online abuse and harassment can do was reported by research from the Victims' Commissioner. In 2019, The Space conducted a small survey of 126 people on the topic of Artistic Freedom and the Internet with Index on Censorship. Our survey's findings remain relevant today and lay out how prevalent and pernicious the issue of online abuse towards artists is today. Key findings include:**

42%

of respondents had received virulent criticism or attacks online as a result of their work, including online abuse, trolling, personal attacks and/or concerted harassment designed to silence.

JUST UNDER HALF

of respondents either Agreed or Strongly Agreed that

"the freedom initially offered artists and cultural organisations to publish their work online has become increasingly limited".

14%

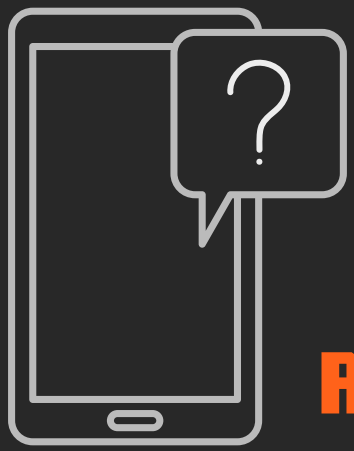
of respondents had had their content subject to calls or campaigns to have the work removed from online platforms or withdrawn more generally.



FEAR OF CENSURE AND ONLINE ATTACK

was significantly higher amongst female than male respondents, and female respondents were more likely to self-censor content as a result.

JUST 17% had known how to deal with virulent criticism or being attacked online.



76% OF RESPONDENTS SAID

"A simple guide to the current legislation, practices by online platforms and rights in this area" would be helpful.

69%



of respondents thought that fear of censure and online attack impacted upon freedom of expression for artists and cultural organisations.



72% said providing **"Online guides/top tips for how to protect yourself/your organisation and content online"** would help.



*An invitation to take part in the survey was circulated via The Space's social media networks and newsletter and Index on Censorship's Twitter account and The Space also shared the link with attendees of its event on Artistic Freedom and the Internet.

Part 2

What do we mean when we talk about online abuse?

Terminology and definitions

Online abuse is a catch-all term that covers a range of digital actions and behaviours. You, your colleagues, those you commission or the organisation you work for may find yourselves the victims of one or more of these.

As these are relatively recent phenomena, the terminology around them is also new and still evolving. Here are some of the most frequently-used terms relating to online abuse (from a list compiled by the Victims Commissioner):

› **Brigading**

Encouraging others to harass someone.

› **Cyber bullying**

Sending, posting, or sharing negative, harmful, false, or mean content to someone with the intent to embarrass or humiliate them.

› **Cyber flashing**

Being sent unsolicited obscene images.

› **Cyber stalking**

A form of harassment which can involve persistent and frequent unwanted contact, or interference in someone's life.

› **Doxing**

The publishing of private or identifying information about you without your consent.

› **Grooming**

Building an emotional connection with a child / vulnerable person to gain their trust for the purposes of sexual abuse or sexual exploitation.

› **Intimate Image Abuse**

The sharing of intimate images taken with or without someone's consent and shared without their consent or knowledge (often referred to as 'revenge porn' or image based sexual abuse).

› **Online coercive behaviour**

Monitoring someone via online communication tools or spyware.

› **Online harassment**

Repeated attempts to impose unwanted communications or contact in a manner that could be expected to cause distress or fear.

› **Online impersonation**

Where someone creates a fake profile pretending to be the victim, with the intent to cause then distress.

› **Fakeporn**

Where pornographic images are digitally manipulated so it looks like the films or images are of someone else.

› **Trolling**

A form of baiting online which involves sending abusive and hurtful comments across all social media platforms.

› **Upskirting**

An intrusive practice, which typically involves someone taking a picture under another person's clothing without their knowledge.

› **Virtual mobbing**

When a number of individuals use social media or messaging to make comments to or about someone.

The UK government adopts the legal principle that what is illegal offline is also illegal online. The Online Safety Act 2023 is a new set of laws that protects children and adults online, which aim to make the UK the safest place in the world to be a child online and to give people more control over the types of content they want to see.

There are a variety of criminal offences that someone may commit in being abusive online. For more information about what behaviours are against the law in the UK, please see Appendix 1: When is online abuse a crime?



Part 3

What does online abuse feel like? Is it a freedom of speech issue?

Personal perspectives


Northern Yemen, 2013

An artist's experience of being the target of abuse online

Yumna Al-Arashi

In 2016, I published a body of work titled Northern Yemen, which depicted powerful Yemeni women in beautiful landscapes throughout Yemen. They were covered in hijabs and niqabs, but still managed to look like superheroes. I made this body of work as a protest to the negative portrayal of the Muslim woman in modern western media. The work went viral.

For the most part, the work was received well but I began to notice something strange: there were a few people who were horrified to see an image they weren't used to: a Muslim woman looking powerful. I started receiving comments about how irresponsible I was for depicting Muslim women with possibility of strength, as if an oppressed woman should only be seen as such. It felt as though these commentators were actually more oppressive than the places these women were from. I ignored the responses at first, but soon they became incessant, angry, scary.

I began panicking, questioning my own work and motives, wondering if these people were right for attacking me. The noise became louder and louder, and moved from just my social media sites to my e-mail inbox. Death and rape threats started pouring in. One person managed to find where I was living and sent me a screenshot of my home from Google Maps, warning me to watch where I slept.

I began removing myself and my work off the internet as much as I could. I found myself immersed in fear and paranoia. I began losing the motivation to make and share my work. This, of course, limited me in many ways. My self-censorship not only broke a stream of my artistic production, but it also created a break in my financial stability. I no longer wanted to create, promote, or interact online. The place that once was the all-encompassing tool for my work became my worst nightmare.

At the time, I was completely unaware of any resources available to artists who experienced this type of harassment and censorship. I believed that if my friends could hardly understand what I was going through, how could any organisations? How could the government? I didn't realise that the threats to my safety were against the law and that I did have options available, resources to take advantage of, and communities to support me.

Instead, I isolated and self-censored while I found ways to heal from the traumatic experiences of being stalked, harassed, and threatened online. While removing myself from the internet created a blow to my career in many ways, I found it to be the only way I could recover from the all-encompassing fear and paranoia that I was mentally submerged in. I found time to heal mentally through therapy and with the support of my friendships and family.

In retrospect, I wish I'd known that there were resources available to me. Furthermore, I wish it were clear, common knowledge that artists do have support. Though our resources and laws might still not be where they need to be, the lack of visibility of the resources that do exist bothers me. If we aren't aware of what is out there and what we have and do not have, how can we ever get better from this point forward? How can we heal, find help, support one another?

I managed to crawl myself and my career out of a dark space on my own, simply because I was lucky to have a support system that gave me strength to keep going. But not everyone is as privileged as I am. The problem and the stigma around it still exist and people are still suffering. This problem must change now.

This toolkit is a project in collaboration with the team at The Space to make sure that artists such as myself know their rights, their options, and the support they can access in times of trouble, as well as showing organisations what they can do to help and support those artists and other members of their teams – both before and during an attack.

An organisation's experience of being at the centre of a media storm

Manchester Art Gallery curator Clare Gannaway speaks to Natalie Woolman about #nymphgate

Background

Leading contemporary artist Sonia Boyce had been collaborating with Manchester Art Gallery team for several months when they decided she would stage a 'takeover' of the space. This followed several months of discussions with staff – including curators, gallery assistants and volunteers – about the role of the curator, how artworks are selected and presented in the galleries and how that shapes cultural identities.

As a result of these conversations, Boyce staged an event in January 2018 that explored gender representations within the gallery's permanent collection. For the event, Boyce invited a group of drag artists to perform in the space and interact with visitors. The climax of the evening was the removal of John William Waterhouse's 1896 painting Hylas and the Nymphs.

In its place on the wall, the gallery explained that it had temporarily taken away the painting and asked visitors for their reactions to the work and its removal. Audiences were invited to respond on post-it notes which were then put on the wall's empty space. The whole evening was filmed as part of Boyce's new film Six Acts which would be shown in the gallery later that year.

One of the visitors to the event reported his discomfort about the removal of the painting on X, at that time Twitter, and subsequently spoke to the press. He said he felt the painting's removal was an act of censorship.

A deluge of press coverage from around the world and a social media storm followed. The Space spoke to Clare Gannaway about her experiences of dealing with this incident. Looking back, Clare said that the response came as a **"complete surprise"**, especially in its tone and volume.

In almost all of the reporting, a lot – if not all – of the context of the event had been shorn from the story, including that it was always intended to be a temporary removal of the painting, albeit open-ended.

The experience from the inside

She described how the gallery was **“bombarded”** by **“every form of communication”** – letters, emails, phone calls, media requests, posts on social media and verbal comments made to staff working in the gallery itself.

Amongst the torrent of social media posts, there were calls for resignations and the gallery’s actions were compared to the behaviour of extremist regimes. Although Clare said she didn’t feel she needed to report anything to the police, she said that **“dark”** things were sent to the team by post that were clearly intended to unsettle the recipient. There was also an incident when someone found and contacted one of Clare’s relatives with a veiled threat.

Much of this behaviour was focused on Clare as the gallery’s curator of contemporary art. However, the gallery’s front of house team also found themselves on the receiving end of verbal abuse about the project.

Clare described: **“One of the things that upset me the most was seeing how some of my colleagues were treated. Many of the people who faced [the public’s anger] – our front of house team – had no choice but to be in the public parts of the gallery or to pick up the phone. It was totally unfair that people came in and were verbally abusive to those colleagues.**

“I feel there are lots of conversations to be had with people who work in those public-facing roles about what they have to deal with – the process with Sonia had already opened up this area of concern – and as a sector we need to talk about this more.”

At the peak of the incident, Clare said it impacted people in every part of the organisation because the story became public and went viral so quickly. Due to the volume of letters, calls and emails everybody was fielding things for a day or two at the height of it. She added: **“I should say it wasn’t all negative – some people got in touch with positive feedback and in solidarity.”**

Emotional and psychological impact

In terms of the emotional impact of the incident, Clare described: **“I must have quite a thick skin. I don’t feel that my mental health was badly affected by it – I had confidence in the decision to do what we did and solidarity with Sonia and those involved from the gallery team. But I understand that for some it would have been – and perhaps was – terrifying and traumatic. Everyone responds to these things in different ways.”**

She stressed that it helped that, because the project had been undertaken as the result of a series of conversations with people across the gallery who had come to a collective decision to remove the painting temporarily, she did not feel alone.

“Teamwork, solidarity and understanding of why you’re doing something is important. If you understand why you are doing something it helps you to feel confident about it, as does remembering that you’re not responsible for the ways that other people choose to behave,” she said.

Nevertheless, she said that some members of the team felt really unsettled by the experience and the most stressful aspect of the incident for Clare was seeing the distress it caused to some of her colleagues.

Managing communication

At the height of the media interest, Clare did a number of press interviews. The gallery also issued a press release and Clare wrote a blog explaining the rationale around the project.

She was advised on how to update her privacy settings on her social media profiles. She told us that she did not respond to posts on social media because she knew it would be **"pointless". "These platforms are designed for conflict,"** she added.

Looking back

Clare emphasised how interesting she thought the project was, and how the public response to it illustrated people's relationship with art and the process of selection and curation. As she described: **"Putting the abusive comments to one side, it laid bare what people think about what we do and also how we live and work in a cultural context of resistance to change, where sexism and racism still persist, and how the media and social media often perpetuate this."**

The experience prompted the gallery to build a closer relationship with the communications team of Manchester City Council (who own and operate the gallery) so that they were across the gallery's aims and vision and the two organisations could work more closely together.

Manchester Art Gallery is also part of the Manchester Museums and Galleries Partnership alongside the Manchester Museum and the Whitworth, and together they set up a meeting in the wake of the 2018 incident. This enabled staff to reflect on the experience, their feelings about it and issues that arise out of being online, including the blurring of personal and professional boundaries.

In terms of how the gallery moved forward from the incident curatorially, Clare said that she and the gallery team proceeded in a positive direction. They continued to have conversations about the gallery spaces and displays that hadn't changed in a long time, how they could evolve in a way that was open and democratic for the public and how the gallery could help to shape cultural narratives that shift the kinds of attitudes demonstrated by much of the abuse.

Indeed, the team included some of the media reporting and correspondence the organisation received about Hylas and the Nymphs alongside Boyce's work Six Acts within the gallery, and archived (both physically and digitally) some of the responses, as a means of capturing this new aspect of the painting's history.

What is it like being an organisation targeted by abuse online?

Rowan Kerek Robertson, Social Media and Digital Content Consultant & former Head of Social Media, BBC Television



Most arts organisations, broadcasters and publishers will deal with contentious content at some point or another, perhaps routinely. Even content that doesn't initially appear very contentious can, now more than ever it seems, get strong reactions.

A 2016 investigation by The Guardian headlined "**The Dark Side of Guardian Comments**" revealed how a minority of persistent posters harass their journalists (specifically female and black writers in this case) with a huge impact on the writers' lives. While 2016 may feel like an age away now, the experiences described by The Guardian journalists could still, sadly, happen today. Online harassment is still happening today and while the Online Safety Act may serve to protect us in some ways, it will not prevent the societal issues which feed into many of social media's problems.

"My life looks really different than it did ten years ago, because of online harassment. When someone comes up to me one on one to talk, I get nervous. I'm like 'Is this the person who said they wanted to rape me last week?' I have a PO box, I don't have a public address listed. I don't check into hotels using my real name or my husband's name. I don't have a public facing calendar for when I do speaking events. In addition, I follow pretty serious security protocols: metal detectors before students can come; not publicising an event that they're hoping to get a lot of people to. The last event that I spoke at, they had a bomb sniffing dog. It completely changes the way that you live your life," one of the journalists reported.



Organisational responsibility

While harassment is often aimed at individuals, the responsibilities of employing or collaborating organisations certainly come into play where people become targets because of their association. As The Guardian is a proactive publisher, which has opened up the commenting facility, or in another instance published the content on social platforms where people can freely comment, the responsibility is direct. Therefore, moderators on The Guardian's website remove comments which cross the line and break their guidelines.

Notably, they have reduced the number of articles they open for comments in recent years and while journalists interviewed for "**The Dark Side of Guardian Comments**" acknowledged the value of open debate and of being challenged on opinion pieces in particular, one of them also said that not having comments on pieces at other publications has "**been lovely**".

Trolling behaviour and hate speech are not limited to the boundaries of one website, and users often follow those being targeted to other online locations. Thinking through possible support and duty of care before a project begins is critical, to minimise the potential for harm.

While there's no easy answer to solving hate speech, support from organisations can be empowering. Is having commentary from users helpful and valuable to the project? Is there a way the organisation can support those dealing with the comments? Journalist Steven Thrasher reports that at The Village Voice his Editor would come on and support him when he was verbally attacked online. The scale of online commenting has changed so it would be hard for the head of an organisation to engage in counter speech in today's world, but the idea remains that support is critical, with the question becoming how can we deliver it at an organisational level?

Privacy settings

As detailed in **Part 5** of this toolkit, encouraging individuals to make choices about their online privacy and security settings is a very good way of trying to **minimise the impact of online harassment should it happen**. This is true generally, as a supportive measure for staff, but where people publicly represent your organisation, it's arguable that there is more of a duty of care in regard to protecting them from potential harassment they may receive because of their role.

When an organisation helps someone step into the spotlight of public attention, there is arguably a significant responsibility to make sure they are able to protect themselves online, especially if their – or your – work may challenge people. It must be started before the spotlight is turned on, so they can make choices about their privacy rather than react to potential harassment. The more contentious the subject matter surrounding them, the more critical it is. Empower your team with easy-to-use guidelines about privacy and security. Be proactive in thinking through the situation with those who you can identify as potential targets. If you don't have the expertise in your team, seek it externally. Include it in your risk assessments!

The value of guidelines

Developing an organisational sense of what is and isn't acceptable can be helpful. The line between negative commentary and harassment can sometimes be blurry, but guidelines such as the **BBC's commenting guidelines** for their own website, which are the basis for moderators making fine-grained decisions about harm and offence, can be a useful tool to help make judgement calls in grey areas. Being challenged is part of our rich creative culture. Being abused, defamed or threatened is not. What would not be acceptable in physical life should not be acceptable online.

Besides content or projects being touch points, organisations can act as a symbol or be a target themselves for various reasons, which may attract attention from bad actors around the world.



Hacking

Perhaps the most common type of attack we hear organisations coming under is hacking, which may result in malware that damages your computers, or ransomware gaining entry to your own digital network. Ransomware encrypts your files and demands a payment to release them. It can be utterly crippling if you can no longer run your organisation. Distributed Denial of Services attacks, which overwhelm targeted servers with huge amounts of disruptive traffic, can also be crippling, with blackmail and activism being motivators.

In the commercial world, the ambition of hackers is often to get peoples' personal details from large databases for criminal purposes. Or conversely, small companies may be hacked because their cyber security is lacking. In early 2024 the UK's Department for Science, Innovation and Technology reported that, **"Half of businesses (50%) and around a third of charities (32%) report having experienced some form of cyber security breach or attack in the last 12 months. Clearly our organisations are not prepared for such cyber attacks."**

Even where an organisation may have good cyber security, often staff are a weak point. Indeed, in April 2020 during the coronavirus pandemic, the World Health Organisation had to contend with an increased number of attacks on their staff. While the WHO itself wasn't hacked, employee passwords were leaked through other websites.

Phishing

Phishing messages have been a common way to gain entry to large organisations over the years, where a legitimate-looking link from what looks like a reputable source actually takes those who click on it to a malicious website that may install malware that gains entry in some way to your system.

Some years ago a phishing email was sent widely to BBC employees. It looked like a real email from someone at The Guardian. Of course, those who didn't think not to, clicked on the link rather than examining it before doing so. Only a few people clicked on it, but their laptops were accessed by the actual authors, the Syrian Electronic Army, who searched for any information they could use to promote their cause. They found some password files and promptly accessed some of the BBC's accounts on X, at that time Twitter, changed the access details so BBC staff were blocked out and posted some tweets for their own ends – weaving in another form of online harassment: impersonation.

For those on the ground, there was then the process of identifying what was happening, trying to assess the damage, getting in touch with Twitter to help and then make decisions about how to clean up.

Tweets posted by the hackers included "**Long Live #Syria Al-Assad #SEA**" and "**Tsunami alert for Haifa: Residents are advised to return to Poland.**" The accounts were quickly restored, with apologies making it clear they had been hacked.

Of course, there are numerous bad actors online and anyone who has ever been part of an emergency situation like this has an idea of the pressure it puts people under.

Proactive preparation

The less prepared people are, the less they've thought about that eventuality happening, and the more panicked the response is while the right people are scrabbled together. But where there is a plan, even if a basic one for who to call together (the Director, the social media leaders, the Head of Comms, those on the ground, those with the technical expertise) and how to reach them, the panic can be minimised and the business of sorting out what to do can begin by convening in one conversation quickly with the appropriate people.

Most online harassment does happen to individuals. In The Guardian's case as referenced above, it's clearly the writers who are targeted. But even where harassment is directed at an organisation, it can be so stressful and emotionally challenging that it feels personal to those who have to deal with it inside an organisation.

This is especially true as attacks are often coordinated, not only for hacking or DDoS attacks, but also for campaigns of hate speech, where sometimes people will gather on the dark or private web. So, the perception can often be for those inside organisations, that enormous attacks come out of nowhere. And the less prepared your team is, the more likely it is that the experience will be one of panic, stress and emotional upset.

See Part 4 for steps that organisations can take now to protect and prepare their teams and see The Space's approach to tackling the issue of online abuse in Part 6.

Part 4

What can we do about it before it happens?

How to do an online abuse audit: A guide for organisations

An online abuse audit is an assessment of your current policies, protocols and preparedness for an attack against your organisation, team members or the freelance artists you work with.

As outlined in **Part 1**, below are just some of the ways that you might encounter online abuse as an arts, cultural or heritage organisation:

- **The organisation is subject to online abuse**
- **An employee is subject to online abuse related to their work for the organisation**
- **An employee is subject to online abuse for external reasons but targeting both work and personal accounts**
- **A commissioned artist is subject to online abuse related to work commissioned by the organisation**
- **A regularly commissioned artist is subject to online abuse for an independently commissioned piece of work**
- **The organisation is drawn into a more generally contentious position online**

The starting point for an arts organisation will be opening a conversation about online abuse and harassment within your team and those you work with. Indeed, thinking through how such an incident could impact your team, the freelancers you work with, your audience and your brand is likely to reveal how holistic your approach to this issue needs to be.

In how you wish to respond and the tone and 'voice' you want to adopt online, your artistic or editorial leaders need to be involved; in how members of your team or collaborating freelancers might be affected, your HR team may need to be consulted; and, assessing your cybersecurity will involve your IT team.

At the beginning of this journey, it is worth considering who is likely to first see or deal with online abuse. It may be a junior member of the marketing team who handles your social profiles, or a freelance artist that you have commissioned at home alone.

As organisations, we have a responsibility to protect those who work for us, especially when we are commissioning their work, or asking them to speak on our behalf. Simple steps such as having policies in place to manage an online abuse scenario if and when it occurs including escalation and response protocols and training are important to make them feel secure in their work.

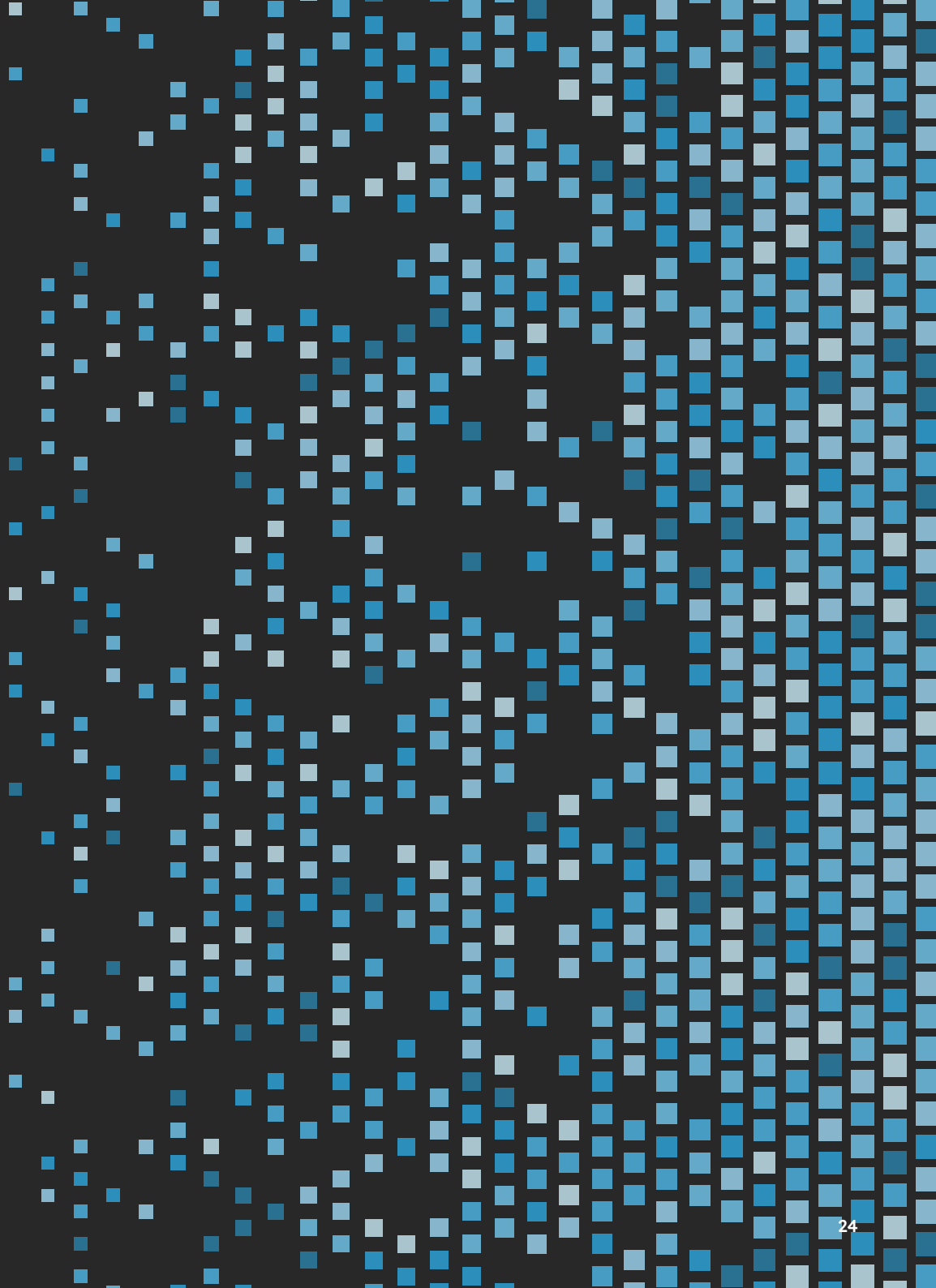
Overleaf are some questions designed for cultural organisations to consider as part of an online abuse audit.

The Space offers a range of support to help arts and heritage organisations plan for and respond to online abuse. These services include risk assessments, consultancy for organisations looking to draw up policies and protocols to deal with online abuse and bespoke training for managers and teams.

To find out more, please email contactus@thespace.org

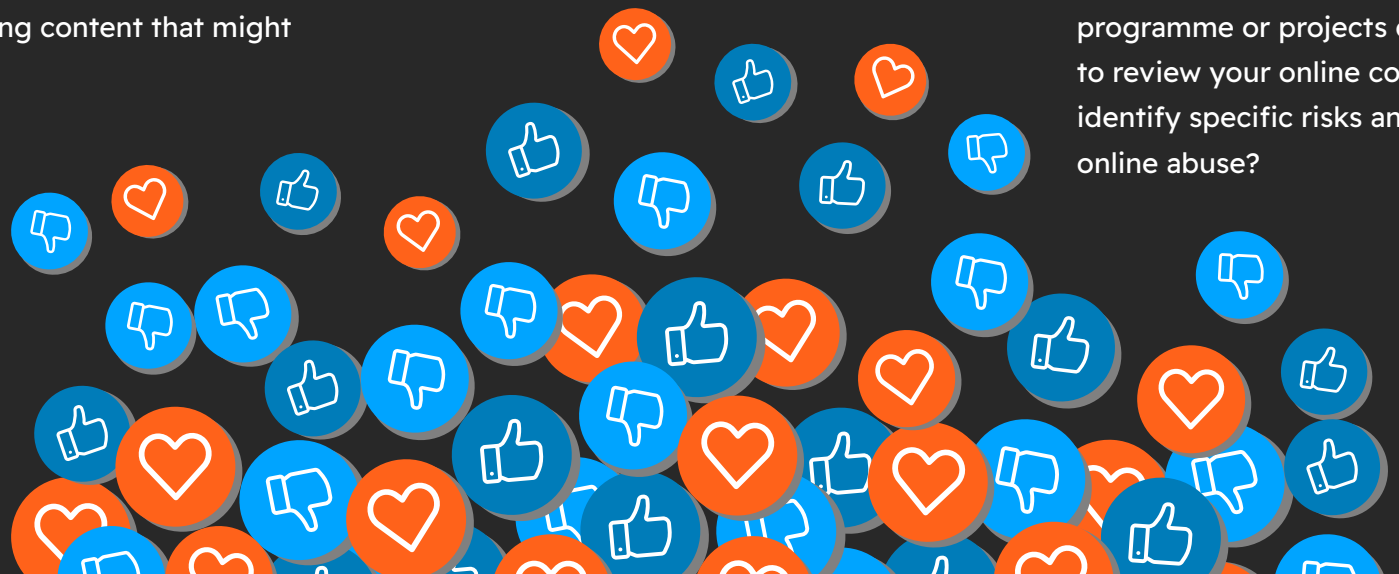
RISK PROFILE

- Are there aspects of your organisation or its activities that might be considered high risk in relation to online abuse? Areas to consider include:
    - Campaigning or supporting causes or themes that might attract online abuse
    - Running performances, events or other activities that might attract online abuse
    - Employing or working with individuals who might be at risk of attracting online abuse
- Given your risk level in the above areas, do you feel you have satisfactory plans and policies in place for the areas identified below?
- Is it clear who in your organisation is responsible and accountable for issues relating to online abuse, digital security and your responsibilities to employees and other collaborators in this area?
- What is your organisation's approach in relation to balancing freedom of speech with the need to prevent online abuse?



SOCIAL MEDIA AND ONLINE CONTENT

- Who is responsible for managing your social media channels and other online content?
- Who can publish content on behalf of your organisation or act as a named representative online?
- How do you manage passwords to access your social media channels?
- Is there a process for changing/deleting user access for publishing content when a person leaves your organisation?
- Do you have an online content policy that addresses tone of voice to be used in online content and when and how to comment about or share third party content?
- What is your process for approving social media or other online content before it is published and for flagging content that might be high risk?
- Have you reviewed the privacy policies, sharing and commenting settings for your social media channels to manage who can see and comment on your content publicly?
- How do you monitor social media, so you might respond in a prompt manner to any negative public comments about your organisation or its work? Do you need to do this outside business hours?
- Have the individuals managing your online content been trained in the issues raised in this toolkit?
- Do those individuals have the skills and experience to take appropriate decisions in higher risk areas or to know when to escalate an issue?
- Do you have a clear process for escalating issues, including readily available out-of-hours contact details for the relevant senior managers?
- In the event that your organisation or a member of your team experiences online abuse, do you have clear communication and response guidelines and do you know when and how to notify the authorities?
- Do you have a policy for employees' personal use of social media, including making references to your organisation/ work, publishing opinions that might bring your organisation into disrepute and use of social media during company time or using company equipment?
- When forward planning your cultural programme or projects do you have a process to review your online content strategy and identify specific risks and mitigations around online abuse?



IT SYSTEMS

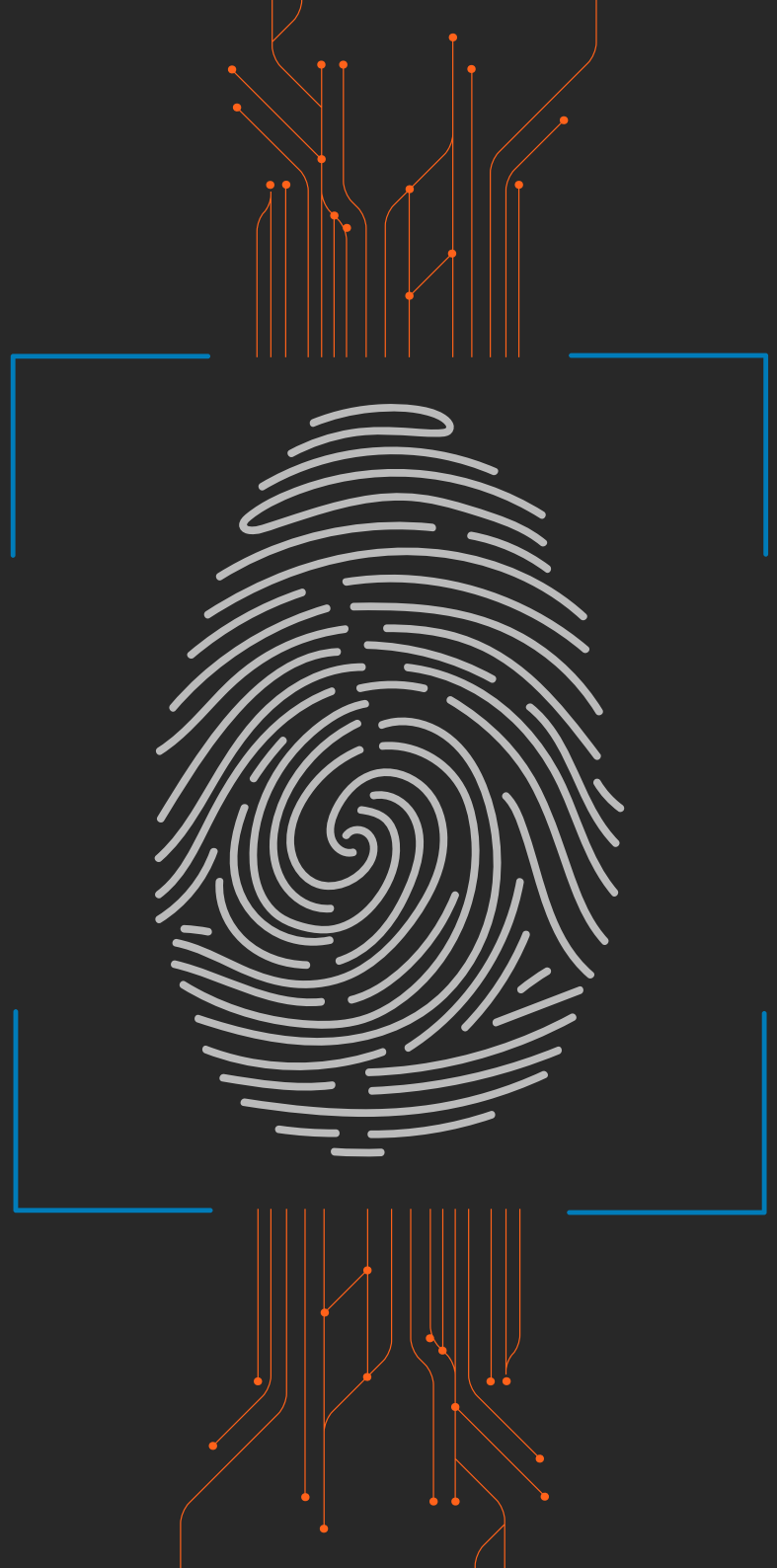
- Do you have legally compliant policies and processes covering data protection and privacy, including GDPR?
- Is the data your organisation stores encrypted where necessary and regularly backed-up?
- Do you have clear policies and secure processes covering your team's access to software and systems, including using secure passwords, password managers and two-factor authentication, where appropriate?
- Do you have up to date anti-virus software installed on the computers used by your team?
- Have your staff been trained in digital security, including how to identify and prevent social engineering attacks on your digital systems (e.g. phishing or similar)?
- Do you have online services that could be vulnerable to a Distributed Denial of Service (DDOS) attack? If so, have you considered defensive measures?

HR

- Do you have policies and processes covering your duty of care in relation to online abuse for employees and artists and other collaborators you may be working with?
- Where you have identified people who may be at higher risk of encountering online abuse, do you provide training and support for them to reduce this risk?
- If people in your team did experience online abuse, do you have guidelines on how you will support them and do you know what resources you might signpost them to?
- What is your approach to identifying staff and collaborators on your website or elsewhere online and publishing personal information or images? Have you secured their permission? How do you balance the risks of this versus the benefits?

FOR INDIVIDUALS TO REVIEW

- Do you use secure passwords, a password manager and two factor authentication where appropriate when accessing your online accounts?
- Have you reviewed the privacy and security settings of your social media accounts recently and are you happy with the settings?
- Have you researched what information is available about you online?
- Are you comfortable with this or do you want to take steps to try to have certain information removed?
- Have you checked whether any email addresses or passwords you use may have been compromised in a previous data breach?
- Is the data on your personal devices encrypted and backed-up?
- Do you have up to date antivirus software on your computer?
- Are you comfortable with the extent to which you separate your personal and professional identity in terms of the online information you share?



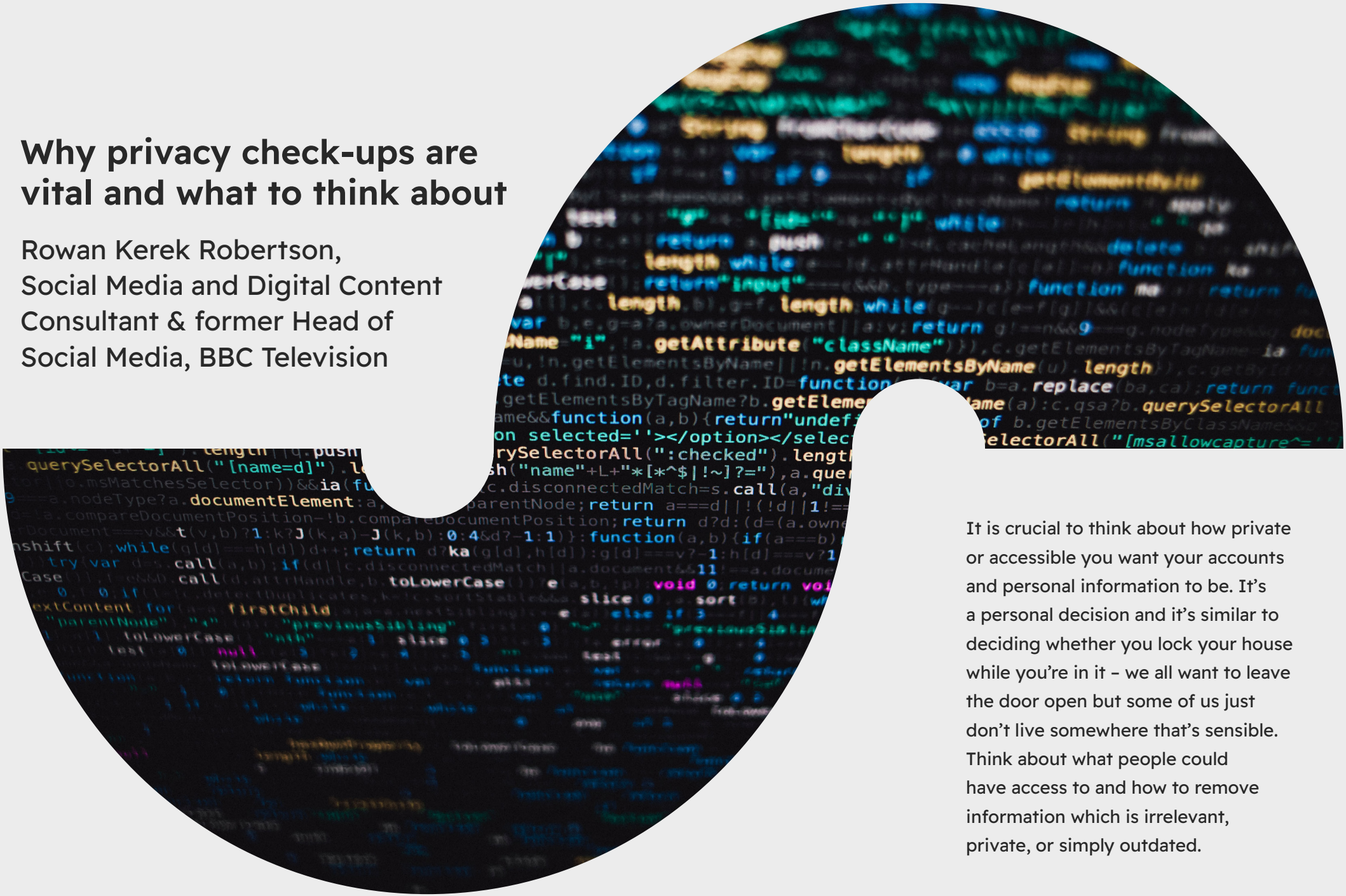
Part 5

What can we advise individual artists and team members?

Privacy settings and what to do when you are subject to an attack online

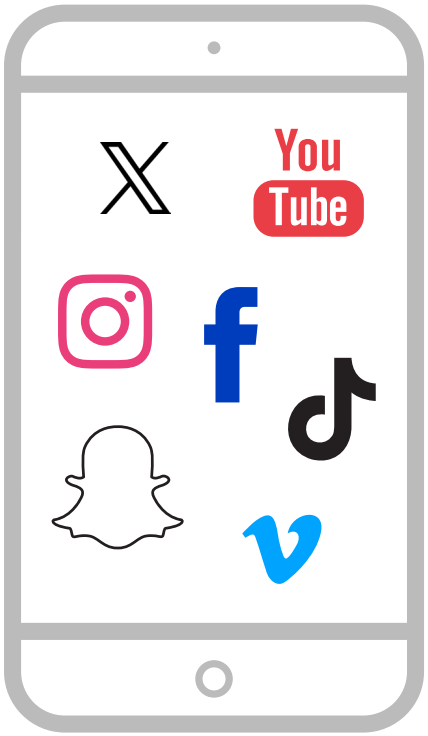
Why privacy check-ups are vital and what to think about

Rowan Kerek Robertson,
Social Media and Digital Content Consultant & former Head of Social Media, BBC Television



It is crucial to think about how private or accessible you want your accounts and personal information to be. It's a personal decision and it's similar to deciding whether you lock your house while you're in it – we all want to leave the door open but some of us just don't live somewhere that's sensible. Think about what people could have access to and how to remove information which is irrelevant, private, or simply outdated.

PRIVACY CHECK-UP
What to consider...



Take charge of your social media accounts

You can make all of your social accounts private if you want to. Go through the settings for each of your accounts to ensure you're happy with what people can see and how people can contact you. In particular, make sure you've chosen settings you're happy with in regards to:

- What you're notified about – turn on "high quality content" filters where possible. On X for example you can choose whether you're notified (or not!) by people you don't know, who don't follow you and those with new accounts etc.
- Whether people can tag you – tagging people on disturbing images is a common bullying tactic. You can change your settings so people can't tag you on images to avoid it.
- Whether your location is shared – there is rarely a need for people to know exactly where you are while you're there. For example, if you like to check in on FourSquare etc, you can do it afterwards.
- Decide who can send you private messages – perhaps only people you follow.

Additionally, try to claim accounts with your name to avoid impersonation, even if you're not going to use them.

Protecting your personal details online

One of the main things to try and protect is your personal information. If you search for yourself whilst you're in the middle of an attack, you'll simply see lots of upsetting information. Instead, search for your information such as your phone number, private email address or real address. Use inverted commas around data which appears in a specific format like your phone number to tell search engines you're searching for something specific.

Unfortunately, personal data can get into the public domain in a number of ways including via the Electoral Roll, Companies House, domain registration or the phone book. It's best to find out what information is out there before you find yourself in the spotlight. To do this, you can use people-finder websites including **findukpeople.com**, **192.com** and **UKphonebook.com**. Notoriously, they're often able to find shocking amounts of information in totally legal ways.

If you find things that you don't want to be public, contact the websites and search engines listing them and ask for them to removed, or use services such as **undoxme.org** or **databrokerswatch.org**.

Think about your accounts

Have different accounts for different purposes e.g. public vs personal activity. Sign up to different accounts with different email addresses for different purposes. Use different images as your social icons to avoid people linking accounts you don't want linked.

Depending on the platform, you often don't have to use your real name on social media accounts. If you're working on a contentious project, you may consider removing links between your physical self and your virtual accounts. This is easier on X but not permitted on Facebook and LinkedIn, although on those platforms you can close down who can contact you.





Protect yourself from hacking

Use 2 stage verification where it's offered, find out more at **twofactorauth.org**. Use strong passwords with services like **1Password** and **LastPass**.

Be conscious of what you share

Personal details, locations, addresses, contact details and photos all offer up information: Be careful not to share "jigsaw" information (about children too), which when put together forms a detailed picture of you, your life and your loved ones. Some people even delete their posts regularly, to simply reduce the trail of content attached to themselves.

Useful tools for removing old content

TweetDelete - an automated plugin to delete old tweets to your liking.

The Verge's guide on How to find your oldest social media posts and delete them

ARE YOU CURRENTLY BEING ATTACKED?

Checklist to get through the Here And Now

Remain Calm. Do not interact!

Don't feed the trolls. Interacting fuels harassment further and gives them more reason to fight back. Take a deep breath and step away from the keyboard.

Take screenshots of everything: Tweets, comments, emails, etc

Remember to take screen shots or print hard copies of abusive posts or messages because your abuser may later delete them so your screen shots may be important evidence if you report the incident to the police, for legal reasons and/or to report users to social platforms.

Make sure to include:

- Date and time
- Type of electronic communication (direct message, posted image, social media comment, etc.)
- Location (name of the website or app)
- Nature of the online incident (a threat of sexual violence, a racially-motivated attack, etc.)

Report abuse to the relevant platform:

- X
- Instagram
- Facebook
- Google

Ask yourself: Do I need to contact the authorities?

This may be your course of action if:

- You've received or been named in direct threats of violence
- An online abuser has published nonconsensual, sexually-explicit images of you
- You've been stalked via electronic communication
- You know your online harasser and wish to seek a restraining order

How can I report online abuse as a criminal offence in the UK?

▶ See **When is online abuse a crime?**

If you feel you are in immediate danger:

If you are receiving verbal, written or psychological threats, threats of a sexual nature, or threats to kill, or racial or religious threats known as 'hate crimes' which you feel put you in immediate danger or at risk, call 999.

If you are not in immediate danger, you can report being threatened:

- By calling 101
- By going in person to your local police station
- By filling in a 'report a crime' or incident form online

Ask yourself: Do I need a lawyer?

▶ If so, please refer to the **Resources section** of this toolkit.

If you feel you are being censored or self-censoring:

Visit **Index on Censorship**'s Arts Censorship Resource Service.

Ask yourself if you would benefit from community or emotional support?

Your mental health and wellbeing is very important – speak to a friend, colleague or support worker. Please refer to the **Resources section** of this toolkit for services that offer support in this area.

Part 6

What is The Space's approach to tackling the issue of online abuse?

For The Space's internal thinking and planning on this issue, we have adopted the following principles that govern our approach. If they are helpful, please feel free to adopt them for your own organisation or practice.



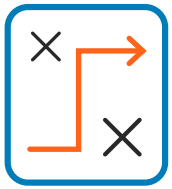
Talk

We will encourage ongoing discussions about the thorny issue of online abuse within our organisation and encourage staff, freelancers and associates to talk about what it means for them and share their experiences.



Train

We commit to training our teams in what online abuse is, what constitutes illegal behaviour and where they can find help and support if it happens to them.



Plan

We will plan for online abuse towards or within our organisation – how these incidents should be handled and escalated and how we will support those at the sharp end.



Share

We will share resources and expertise with other individuals and organisations within the sector on this topic so that as many people as possible know where to find advice and support.

Part 7

Resources

Resources and helpful links

Legal resources

- Find a legal aid adviser
- Citizens Advice Bureau can offer general advice and refer on for legal support
- Index on Censorship's support is available to anyone in the UK cultural sector (employed or self-employed) who is facing an issue of censorship
- Rights of Women offers advice to women about the law and their legal rights in England and Wales

Community Guidelines resources

- BBC rules for commenting and uploading
- Guardian's community standards
- Southbank community guidelines
- Bush Theatre social media guidelines

Mental health resources

- Samaritans offer free support 24/7 if you call 116 123
- Victim Support offers free and confidential support to people affected by crime or traumatic events in England and Wales
- The National Stalking Helpline gives practical information, support, and advice on risk, safety planning and legislation to victims of stalking, their friends, family, and professionals working with victims: 0808 802 0300
- National Bullying Helpline offers practical advice for children and adults dealing with bullying: 0845 225 5787
- Support Line provides a confidential telephone helpline to anyone on any issue, but is particularly aimed at those who are socially isolated, vulnerable, at risk groups and victims of any forms of abuse: 01708 765 200
- The Mix offers support for under 25s including victims of cyberbullying

Proactive planning resources:

- A US-based site, Technology Safety has been compiled for people who have suffered online harassment. It features a lot of practical guidance including how to take a screen grab and how to limit location information on your phone.
- Secure password managers include LastPass and 1Password and many others.
- Social Misfits Media developed this flowchart for how to deal with harassing behaviour online.

Reporting

- Bullies Out is a site aimed at young people but useful to all. It details how to report bullying or abuse to the main social media platforms.
- The Report It site allows you to report hate speech to the police online, as well as giving lots of other information about hate crime.

What to do if you're harassed online:

- Right To Be's aim is to to build a world free of harassment, training "hundreds of people to respond to, intervene in, and heal from harassment". It offers guides, research, workshops and training on many areas of safety, dealing with harassment and how to support people.

Further reading on free speech issues

- David Kaye: Speech Police: The Global Struggle to Govern the Internet
- Nadine Strossen: Hate: Why We Should Resist It with Free Speech Not Censorship
- Article 19 - Responding to hate speech with positive measures – A case study from six EU countries
- United Nations - Freedom of opinion and expression

The Space offers a range of support to help arts and heritage organisations plan for and respond to online abuse. These services include risk assessments, consultancy for organisations looking to draw up policies and protocols to deal with online abuse and bespoke training for managers and teams.

To find out more, please email contactus@thespace.org

Appendix 1: When is online abuse a crime?

The UK government adopts the legal principle that what is illegal offline is also illegal online. There are a number of criminal offences that someone may commit in being abusive online that fall under different pieces of legislation. The Crown Prosecution Service lists the following on its **cyber crime page**:

Hacking is the unauthorised use of or access into computers or networks by using security vulnerabilities or bypassing usual security steps to gain access. Criminals may hack systems or networks to steal money or information, or simply to disrupt businesses.

Malicious software - or malware - can be spread between computers and interfere with the operations of computers. It can be destructive, causing system crashes or deleting files, or used to steal personal data. Viruses, worms, Trojans, spyware and ransomware are all types of malware.

Distributed Denial-of-Service (DDOS) attacks are where more than one, and often thousands, of unique IP addresses are used to flood an internet server with so many requests that they are unable to respond quickly enough. This can cause a server to become overloaded and freeze or crash, making websites and web-based services unavailable.

Social media offences

Trolling is a form of baiting online which involves sending abusive and hurtful comments across all social media platforms. This can be prosecuted under the Malicious Communication Act 1988 and the Communications Act 2003.

Online threats could take many forms including threats to kill, harm or to commit an offence against a person, group of people or organisation.

Disclosure of private sexual images without consent – so called “revenge porn” is a broad term covering a range of activity usually involving an ex-partner, uploading intimate sexual images of the victim to the internet, to cause the victim humiliation or embarrassment. It is a criminal offence to re-tweet or forward without consent, a private sexual photograph or film, if the purpose was to cause distress to the individual depicted.

Online harassment can include repeated attempts to impose unwanted communications or contact in a manner that could be expected to cause distress or fear.

Grooming refers to the actions of an individual who builds an emotional connection with a child to gain their trust for the purposes of sexual abuse or sexual exploitation.

Stalking online is a form of harassment which can involve persistent and frequent unwanted contact, or interference in someone’s life.

Virtual mobbing takes place when a number of individuals use social media or messaging to make comments to or about another individual, usually because they are opposed to that person’s opinions. The volume of messages may amount to a campaign of harassment.

Source: Crown Prosecution Service

However, the law around online abuse is still in the early stages of definition and action. The matter can be complicated further if it is not clear who or where the attack is coming from.

Ask the Police explains how the misuse of social media messaging can be viewed into harassment under the law:

> **"If a person sends threatening/abusive/offensive messages to another person via Facebook, X (formerly Twitter), or any other social networking site, they could be committing an offence. The most relevant offences are 'harassment' and 'malicious communications. The offence of 'stalking' may also be relevant if a person is being targeted persistently by someone across various social media accounts, along with any other repeated, obsessive and intrusive behaviour, that causes the person alarm and distress.**
>
> **For harassment to be committed, there must be a 'course of conduct' (i.e. two or more related occurrences). The messages do not necessarily have to be violent in nature but must be oppressive and need to have caused some alarm or distress.**
>
> **If there has only been a single communication, which would be insufficient for the offence of harassment (above), there could be an offence relating to malicious communications. For such an offence to be committed, a message must be sent to another person (or sent via a public communications network) that is indecent, grossly offensive, obscene or threatening/menacing."**

However, often harassment is left to be dealt with by the platforms where the harassment occurs, whether social media or email providers. **Find out more here.**

This toolkit was shaped by conversations with a steering committee of artists and industry professionals. Many thanks to those who contributed: Yumna Al-Arashi, Manisha Ferdinand, James Mackenzie-Blackman, Simon Mellor, Tonya Nelson, Dr Linda Papadopoulos, Jo Verrent.

Updated in 2024 by Rowan Kerek Robertson.

The Space is a commissioning and development agency, founded by the BBC and Arts Council England, committed to supporting and facilitating the UK cultural sector to realise its digital ambitions. It does this through the commissioning of arts projects, supporting arts and cultural organisations to develop their digital plans and activities and offering training workshops, advice and resources. The organisation has supported the delivery of more than 400 digital projects commissioned with online and broadcast reach exceeding 50 million sessions.

Edited by Yumna Al-Arashi

the space

LOTTERY FUNDED

Supported using public funding by
ARTS COUNCIL ENGLAND