West Yorkshire
Violence Reduction
Partnership

West Yorkshire
Health and Care Partnership

TRAUMA-INFORMED USE OF TECHNOLOGY IN BUSINESS,SME AND VOLUNTARY-SECTOR ORGANISATIONS

Guidance

Authored by:

Catherine Knibbs

On behalf of the West Yorkshire Adversity Trauma and Resilience, Digital Workstream

Introduction

Technology is everywhere and is an essential part of our work and personal lives. Because we often use it without consciously thinking we might be at risk of many cyber incidents and online harm issues.

This document is the first of its kind in the UK to provide a trauma informed approach to thinking about our digital use in both services such as policing, housing education and personal use.

Today, we are so used to using technology that we might not give a thought to the fact that we are continuously online. In fact, young people do not make this distinction at all. The way we engage with and through technology has been changing and will continue to do so as Artificial Intelligence evolves. Using a smartphone to access information, for example, can feel like a different experience from doing the same on a desktop computer. And, crucially, communicating with people through text or direct messages on an app and engaging in interactive relationships online is a world in which we're still getting to grips after almost half a century.

There is much potential and excitement associated with this new reality, and certainly many more changes to come. As use of the technology expands, so does the potential for it to create what we now call online harm and result in what Catherine Knibbs describes as cybertrauma. We've seen this happen increasingly over the last decade, with several deaths linked to use of, and with people in, the online space.

It has taken some time in the UK to pass a law aimed at reducing these risks. The Online Safety Act (2023) came into force with the aim of making the internet, and online spaces more broadly, a safer place in the United Kingdom, especially for children.

However, we believe that the Act is not wide-ranging enough to capture many of the harmful impacts that we would classify as traumatic when using the ATR (Adversity, Trauma and Resilience) programme framework.

This document represents a first effort in providing guidelines and direction to help the people of West Yorkshire become trauma-informed in the context of digital spaces. It is intended to be especially applicable to the use of technology in workplaces and specific sectors, and provides some thinking for personal use of technology so you can help yourself stay safe online. In fact, this is the first set of guidelines of this kind in the UK, so West Yorkshire is very much in the forefront on this topic. The document is necessarily limited in scope at this initial stage. Working directly with our strategic partners, statutory and third-sector services, and businesses that are part of the ATR community, we will create more detailed and specific guides as we develop our understanding and expertise. This guidance document is broken down into short topics, each about a specific area of online and technology-related spaces.

Further information will be available on the West Yorkshire Health and Care Partnership and West Yorkshire Violence Reduction Unit

The Digital Stream

The Digital Stream provides consultations, guidance and information on trauma-informed use of social media, email and text-based communication between businesses, service users, customers and the public (including via websites).

This information is shared with the ATR network to reduce the risk of online harm leading to Cybertrauma®. Cybertrauma refers to any trauma arising from interactions between people using internet-enabled devices.

What do I need to know to be trauma informed in the digital spaces?

Throughout this document, you will be guided to think about your communication systems in your business or service and how they might create, facilitate or impact a person when you are using technology to communicate with them, for example. The document will provide guidance about how to think about your systems and what you may need to do in order to reduce the likelihood of this occurring, and what online harm policies, procedures or systems you may want to use to minimise and mitigate harm (beyond the necessary ones provided by your company, for example, the NHS using Microsoft Exchange systems).

The document is not able to offer guidance on specific systems, as technology is both broad in types of devices and software, and some services are overseen by an IT department, such as the ICB, for example. This document is primarily concerned with how, when and who the communication takes place with, and what considerations your business, organisation or service needs to implement, following both lawful legislation and guidance from Catherine Knibbs' approach to trauma-informed technology use.

Why trauma informed digital practice falls under DPA, privacy and Cybertrauma® thinking.

In short, communications that take place via technology have the potential to cause, facilitate or retraumatise individuals if care is not taken to create a set of policies and procedures that are informed by an ethical and trauma-informed lens. Many services are, for example, using automated communication processes to contact the people they work with, which can become an issue that creates unintended trauma. Over the years that technology has been introduced to business, consideration for contingency plans, communication systems and the 'how we do' of technology communication are often not created for several reasons. This document will help you think about the use of technology with and for human connection, rather than the approach of the technology itself. For example, how do we conduct business if the landline or internet is not working?

During the 2020 lockdown period, technology became a lifeline for many people, yet in this period of time there are many harms that took place through and with technology that have still to be acknowledged, worked with or even written about, so that we can protect people in the future from these issues. The document will help you understand the need for solid and ethical data protection processes beyond that of the legislation (Data Protection Act 2018), to enable you to show the people you work with that you think in a trauma-informed manner when using technology for your business, service or organisation.

What do we mean by technology?

"Technology" is often used as a catch-all word to encompass the equipment we use to connect with others by being 'online'. It includes the devices we use, such as computers, smartphones, and the software (or apps) installed on them.

How do we use technology at the ATR?

The West Yorkshire ATR Programme is part of the ICB and, because of this, the systems we use are overseen by the IT department, meaning that each person within the ATR Programme who has or uses their technology has a unique login, password and email system, and has cybersecurity systems in place to stop cyber attacks from criminals.

The West Yorkshire ATR Programme itself has a website providing information, news and contact details. Our staff use email to communicate with clients, suppliers and other staff members. We have apps that provide services to individuals and businesses. We also have a social media presence, and we interact with clients and interested parties through these channels. In short, the harm is likely to occur through the humans using the system and something they might do, say online, write or send through those systems.

The NHS, ICB and ATR Programme all have adequate physical, cyber-secure and standard operating procedures for 'use' of the technology in terms of making sure data is not leaked, hacked or accessed, but as of yet do not have an ethical use of technology and trauma-informed policy for how the technology is used by humans to communicate with humans, because even we are learning about what we need to do.

As you work through this document, you may identify points where an ethical technology consultation or assessment is required.

In these instances, we would direct you to our Digital Stream Lead, Catherine Knibbs, who has authored this guidance and provides the expert advice that underpins it.

This approach ensures we are consistently informed by best practice and enables West Yorkshire to remain at the forefront, both regionally and nationally, in embedding trauma-informed thinking into the use of technology.

As you read through this document, you will find a brief overview of each area of concern in today's tech landscape, and hopefully gain an understanding of the potential for what we call "Cybertrauma®". The document should act as a pointer in looking to develop a more trauma-informed approach to the technology spaces in your organisation.

Data protection and information security

It is important to protect people, their information (and dignity) by adhering to legislation about how we deal with the information they share with us, called ‘data’. Correct handling of personal information that is kept on an organisation’s system is more than just good practice: it is addressed in UK law.

In 2018, the UK Data Protection law (DPA 2018) was updated from its 1998 version. Much of the conversation surrounding this update centred on what is known as GDPR (the General Data Protection Regulation, EU version), which was established to protect the data of individuals within the EU. Although the UK has left the EU, the principles of GDPR are still enshrined within the DPA 2018 under the UK GDPR version.

However, services and businesses often misunderstand their obligations under the Act. They might think that applying a GDPR training certificate to their business, or requiring a member of the team to take some training, would be the end of the matter. In fact, good practice around the handling of client data needs to be embedded and taken from the entire Data Protection Act, not ‘just’ GDPR, throughout an organisation, beginning with the people who work there and extending to the policies that underpin how the organisation collects, saves, uses and stores data, even if it were on the back of a napkin, for example. Failure to do so can lead to emotional, psychological and repeated harm, or end in tragedy. Leaked or hacked data can be extremely compromising for a person affected. There is evidence of people ending their own lives as a result of information being threatened with exposure online, and crime is increasing, with people being blackmailed for this not to happen.

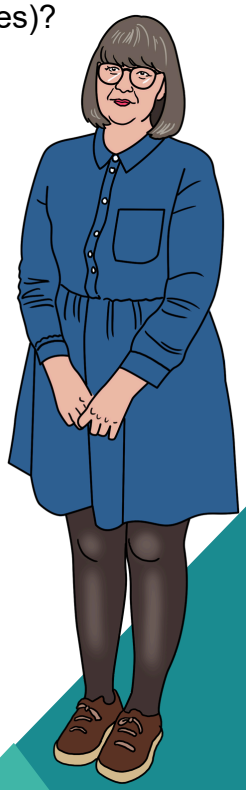
Data protection is the backbone of ethical use of technology, but also includes the pen-and-paper versions that we might write, carry or even scan onto our technology systems. For some professions, they might record audio or take photographs on a device such as a smartphone.

A few things to consider in your organisation:

Do you have a policy for data collection and processing that includes devices not issued by the organisation?

Are you using services that can be seen by technology companies (e.g. cloud back-ups / message reading) when communicating with your customers, service clients or patients?

Are you collecting data on technology and explaining all system risks to the people you use technology with (e.g. video conferencing, age-appropriate systems such as for young people and age-rated services)?



Cybersecurity

This topic follows on from our discussion of data protection. Cybersecurity is, similarly, about how an organisation remains fit for purpose in a digital age. In some services, such as the NHS, this is controlled by the supplier and is installed on all employees' technology. However, this is not something you may have considered on your personal device, which you may be using for work-related purposes.

According to the UK's National Cyber Security Centre (NCSC), "Cyber security is how individuals and organisations reduce the risk of cyber attacks." So, this is about an organisation protecting its own information, as well as that of its clients.

Small and medium enterprises will often take the NCSC's "Cyber Essentials" training and display the certificate on their website or publicity material. Sadly, too few go any further than that, or in some cases only one person in the business takes the course and this is applied to the whole company. Many fail to understand why cybersecurity is of the utmost importance in a digital age: they haven't considered the consequences should a "bad actor" break into their systems. These outcomes can include disabling your website and/or your internal systems, and hacking into your organisation's client or financial data, for example.

"Social engineering" is a term used for malicious activities whereby users are tricked into making security mistakes or giving away sensitive information that allows hackers into your devices and computers, and it is a big business nowadays. It's often taught as part of a cybersecurity course, but when this is seen as a yearly tick-box exercise, carried out as a necessary and often boring part of the role, the fact that criminals, called 'bad actors', are continuously trying to hack into your emails, social media and files is promptly forgotten. Bad actors know that the organisations that take cybersecurity seriously, and make it a priority and everyone's responsibility, are in the minority.

If you want to learn more about data protection and cybersecurity, there are plenty of resources, including the NCSC (https://www.ncsc.gov.uk). Although it's easy to find yourself overwhelmed with these subjects, it's worth keeping up to date with regulatory changes and threats to you and your business. As a trauma-informed organisation, protecting the digital aspect of what you do is as important as how you work with people.

A trauma-informed audit in the data protection and cybersecurity space is well worth the time and effort if it results in a regularly updated plan of action applied to those you serve.

Examples of communication issues to consider when thinking about ethical and trauma-informed use of technology within your business or service.

This section highlights key considerations, prompts for reflection, and practical examples of how online harm can occur. It is designed to help businesses recognise risks and impacts that may not be immediately obvious, but which can significantly affect people's safety, trust and wellbeing.

Devices in business

In these days of portable technology, it is common for people to use work devices at home and home devices at work. This makes it all the more important to have well-considered organisational policies to protect data, as well as training about remote access to certain types of information. Policies will have to be based on an understanding of what devices are being used and what information is shared between them (such as work emails on a personal phone if outside organisations such as the NHS, policing or housing, for example). There will ideally be acceptable use policies, social media policies, and good data hygiene practices that are overseen by a competent IT policy.

Devices must be protected from access by other users to prevent data breaches and accidental sharing of information to other devices. Virtual proxy networks (VPNs) are an excellent means of protecting both work and personal devices.

Customer spaces

On websites, or any other online spaces through which an organisation communicates with its service users or clients, age assurance policies may be required and must be in place where necessary and in line with the Online Safety Act.

Reputable website hosting companies are a must. Along with designers, businesses can ensure their websites collect only necessary information, usually for analytical purposes or to make the website work, and this must be communicated to visitors to the site clearly, with choices such as declining cookies (if enabled). A great way of showcasing trauma-informed data protection practices is to deliberately dispense with the kind of tracking information that could affect visitors' privacy rights or inform their internet provider of the sites they visit.

This also ensures accountability under the Online Safety Act and the Digital Safety Act now in force. If there is an area of the site that requires age verification, for example for a certain training course for adults, then it is imperative that the mechanism for this is compliant with privacy and data protection laws.

Machine learning and AI

Technology is constantly evolving and the landscape changes rapidly. As we learn more about technology and the way it is used, our trauma-informed guidance will be updated. New developments, such as machine learning, large language models and artificial intelligence (AI) software, will have implications around data protection, violation of privacy, facial recognition, age assurance processes and more, and we are always learning about new issues as they arise.

AI software is already being used in back-end spaces, such as websites, and is now also being deployed by individual users, including staff members and practitioners within organisations, for many different purposes, often enabling them to be more productive. It is clear that the terms and conditions of its use are rarely fully understood, let alone how it is integrated with third-party software, which could be reading or collecting the data for other purposes; for example, some AI chatbots collect data to train other systems. Often, it is used in settings in which consent of all parties present has not been sought. An example of this is during video conferences, where conversations might be confidential: there is a way that the conversation can be recorded, and risks begin if it is then not kept securely.

There is no national ethical policy around the use of AI products, nor any organisation to oversee it (beyond Data Protection laws and the Online/Digital Safety Acts). This document represents one early attempt to initiate a discussion about a trauma-applied and ethical approach to the use of AI software in settings in West Yorkshire.

We need to develop best practice for the use of AI bots in place of human-to-human contact (such as a chatbot on a website). AI is not trauma-informed and, as of now, there are no specifically trained models for many of the services this document will be applicable to. AI chatbots, for example, may give advice that could potentially result in a person ending their life, as AI provides logical answers and not those trained on safeguarding or even being able to recognise many of the issues we humans can intuitively see and hear. Therefore, there is a risk that its responses and advice will be abrupt and, furthermore, it might fail to identify critical safeguarding, risky or dangerous aspects of the conversation taking place. As such, AI is not appropriate for crisis work or mental health interventions unless specified and approved by a service such as the UK Organisation for the Review of Care and Health Apps (ORCHA).

Essentially, for the time being, AI should be avoided in most settings. We need to wait until adequate guidance is in place, with an ethical overview and robust evidence that its use conforms to the values of a trauma-informed approach such as that of the ATR.

New realities

There are exciting technological developments around immersive technologies: augmented reality (AR), virtual reality (VR), extended reality (XR) and mixed reality (MX). As with all new developments, it is imperative that trauma-informed considerations and due diligence are brought to bear in any decisions about their use. A key concern here is that this environment is much more intrusive than services delivered via 2D technologies such as video calls or telephone calls.

Virtual realities impact the recipient at a bodily sensation level, can be disorientating, and can cause motion sickness, as a few examples of how immersive they can be. There is also a risk of physical injury from cumbersome headsets, or if the user is physically vulnerable (e.g. their build or muscular presentation, such as a child with growing bones and muscles, or on account of age or illness).

Virtual reality has only recently acquired the potential for mainstream markets, and no standards exist around its design or use, nor for its deployment in training or mental health settings. No aspects of any education or training must be trauma-inducing, which can occur through both the content and the immersive environment re-enacting a situation that a user may have encountered before, as they may forget they are using a VR headset, for example.

Support and use of VR in West Yorkshire for any VR / AR / MX experiences should be thoroughly thought through and approved using the trauma-informed knowledge of the Digital Stream.

See further: Monique Hill, Triton Ong and Catherine Knibbs, White Paper: Mental Health and VR Research (MHVR International Coalition, 2024).

Stimulating and re-encountering traumatic content: immersive technology

Certain educational programmes place the user in a real-life scenario in which they have a first-person, or “bird’s-eye”, view of an event, the so-called “immersive training experience”. As an example, they might have the impression that they’re on the end of a plank with a large drop beneath, or in the sea with a shark, or in a scene of domestic abuse. Such material has the capacity to cause high levels of distress, even rendering the viewer paralysed by fear if the stimulation is too intense. If the viewer is exposed to a violent, aggressive or distressing situation in such a medium, it could lead to a feeling of powerlessness, or a “bystander effect”, meaning the user often forgets they have the ability to remove a headset, leaving them in a situation they cannot escape. This distress can continue once the headset is removed.

As has been reiterated throughout this document, delivery of material without trauma-informed consideration can result in Cybertrauma®, and immersive experiences have more potential than most to be a cause of this, with distressing symptoms more likely to persist afterwards. The trauma-informed language provided by the West Yorkshire ATR Programme is a necessary component within this new technological environment. A useful maxim when considering the use of such technologies is: just because we can does not necessarily mean we should. If we do not have evidence that something is not traumatic (e.g. robust data from clinical trials to support the use of such technology within service delivery or education), nor evidence of complaints about these interventions if such feedback is not offered or sought, then we should avoid using these immersive trainings until we know more. This is ultimately what being trauma-informed is all about, especially when using technology interventions and immersive training.

Social media

1. Social media for service delivery: age restrictions

The key challenge for organisations that use social media apps as part of service delivery (for example, WhatsApp) is to ensure that age assurance and guidance are adhered to. Making sure that such spaces are not being accessed by children under the age of 13 without explicit parental consent is an important part of trauma-informed practice, unless when following the GDPR and providing a counselling service, for example. Parental consent must also be sought when it comes to headset display units and means of access in all settings, for example education or health, and with all forms of devices such as computers, laptops and tablets. Note that many of these devices can allow children onto social media (and other age-gated services). Therefore, only use these services with children and young people when they are of the age of consent for data processing reasons, or if the service suggests older ages for use.

For children over 13, organisations need specific data protection assessments and policies, and e-safety and digital safeguarding policies for each social media app used in service provision for children, bearing in mind that the ages at which children can legally access the various apps and platforms can also differ.

For children under 13 who are being engaged with online for the purposes of counselling, for example, there must be adequate pre-audit policies, safeguarding and trauma-informed processes in place. Provision of services via these spaces must follow the Children's Code as laid out by the ICO (Information Commissioner's Office.
(https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code).

1.2 Social media: Use of children, young people and vulnerable adults on your marketing, social media content

Very careful consideration must be given to the use of children, young people or vulnerable adults in your social media content for use by your service.

You must provide a clear and comprehensive guide and assessment justifying the use of children or young people under the age of 18 in any of your marketing material or social media content, and this must favour the data protection laws of the country you are in and those in which you will share the content. This will require an understanding of global protections for children and their images and voices, and the protection of a child's content and data (such as their face or voice) that can be targeted by cybercriminals and used or manipulated for other purposes. If in doubt about how to protect such content, the advice is to refrain from doing so.

Consent cannot be given for children under 13, and so if using parental or loco parentis consent, there must be a policy for the child's data upon them reaching the age of consent in data (13) and legally (18), enabling them to request the removal and deletion of that data. Bearing in mind that images and voices of children can be used for sexual purposes, used by AI systems, and that other important facts about children can be collected by bad actors to target them at a later date, in most cases the advice is to refrain from using children's data for your content or marketing.

Social media use by staff members

Many organisations have in place an “acceptable use” policy with regard to their employees’ use of social media. Bear in mind that this is less likely to be the case in the voluntary sector, and acceptable use of social media may reflect the organisation’s social media profiles and accounts, but may not hold up for individuals where they have personal social media accounts. It is worth considering what you expect from employees, associates and volunteers who represent your service and what you can ask of them outside of work; however, there are reasonable requests you can make when they publicly state on social media that they work for or represent your service.

The issues that arise here concern professionalism online, freedom of expression online and adhering to trauma-informed practice while acting in a personal capacity online. The nature of online activity means that the lines between work and personal spaces have blurred, and the content we create on our personal accounts can potentially find wide exposure, including among not just co-workers but higher management and clients we work with.

Failure to maintain online professionalism risks issues such as reputational damage to the writer of the content, as well as the organisation as a whole, potentially affecting both co-workers and service users. For an employee of an organisation with a policy or code of practice around trauma-informed language, “online professionalism” must also comprise trauma-informed considerations. The challenge is that such constraints must be balanced with the social media user’s right to freedom of expression, an ongoing ethical and moral dilemma which we see played out constantly in contemporary news stories.

In practice, many people express opinions online and sometimes may be speaking from a position of trauma, or perhaps reactive emotion themselves, especially in social media spaces, that may not meet with their employer’s approval, taste or opinions about subject matter, but in most cases no law has been broken. Any attempt by an organisation to moderate such behaviour in compliance with trauma-informed practice is a potential ethical minefield, but a well-written acceptable use policy can foreground the issues and start the conversations.

The recent changes to the Online Safety Act identify certain harmful content as a priority area to be overseen by law, for example the sharing of named illegal content online, and this is a useful place for an acceptable use policy to start. Misuse of business property or communications technology should also be included, and this is a legal framework that can be added into your policies.

Bearing in mind that we recognise the right to freedom of expression on social media, in order to minimise discord and conflict we should also apply a trauma-informed lens when it comes to reprimanding, punishing or excluding those who have committed (what are seen as) offences when no law has been broken. In cases of online harm occurring through communications and posts online by members of associated staff, volunteers or employees, it may be worth considering restorative processes as part of your policy.

The ATR Programme is continually updating its understanding of the harms that derive from the use of social media. As part of its education around online harms, social media training and Cybertrauma® is available through Catherine Knibbs directly.

West Yorkshire
Violence Reduction
Partnership

West Yorkshire
Health and Care Partnership

For more information contact us in any of the following ways:
caroline.andrews16@nhs.net
Call us 01924 317659
@wypartnership
www.wypartnership.co.uk