ALL RISE

SAY NO to Cyber ABUSE

Guidance on Cyber Abuse in the Workplace - NHS

A Draft Proposal

Authored by:
All Rise Say No To Cyber Abuse

Guidance on Cyber Abuse in the Workplace – NHS

INTRODUCTION

This Guidance sets out the position across all NHS organisations of a zero tolerance of cyber abuse. As one of the largest employers in the world, the NHS takes the responsibility as a national and international role model in Human Resource Management seriously, and acknowledges that by leading on Guidance regarding the principles of addressing Cyber Abuse we can not only influence the quality of online responsibility in communication within our service, but inspire other organisations to raise the profile and quality of communication online.

This document defines our commitment as employers to staff care, and in turn that of our service users, and the collective responsibility of all staff. It defines the actions necessary to protect, support and promote the wellbeing of staff, including stating the consequences for abusive behavior perpetrated across all digital environments.

WHAT IS CYBER ABUSE?

Cyber abuse is any form of harassment, bullying, trolling, vitriol, discrimination, intolerance or hate expressed online or digitally that embarrasses, hurts or intimidates another person. This online and digital environment encompasses websites, social networking sites, chat rooms, message boards, webcam use, phone apps, instant messaging, email and text messages. Cyber abuse can be perpetrated in many forms e.g. via comments, posts, images, memes, videos, use of personal information and pressure to join or leave online environments. A person perpetrating or perpetuating cyber abuse can do so anonymously or as a known person to the target of abuse, and is commonly called a 'troll'.

Examples of Cyber Abuse include:

- Discriminatory, offensive, derogatory, obscene, libellous, threatening, insulting, malicious, intimidating, harassing, abusive and otherwise inappropriate online postings, comments, photographs through cyber communication during or outside working hours.
- The uses of information and communications technology to support deliberate attempts to hurt, upset, embarrass, undermine, humiliate or denigrate another person.
- Sending abusive emails, IM (instant messages) or text messages
- Posting abusive comments, photos on social media such as Facebook, Twitter, Instagram or in chat rooms.
- Misuse of portable communications devices that are issued by the organisation.
- Excessive Internet usage, or non-permissible internet access and accessing inappropriate material via the organisation's systems.
- Hacking into people's accounts and stalking people on social media.

OUR COLLECTIVE RESPONSIBILITY ONLINE

The state of our workplace digital and online communication, and the Internet as a whole, is the responsibility of all of us. The modern workplace environment is by no means confined to the immediate physical surroundings of the work environment. The moment we express online we engage with the potential of over 3 billion online users having access to what we share.

Evidence of the harmful human toll of cyber abuse is growing, its effects including, anxiety, depression, self-harm and suicidal ideation. As a minimum, the standard of our behaviour in our digital environment should be no different to that of our behaviour offline. But there are in fact greater responsibilities that must be considered when it comes to our online behavior. For example, the potential is great for comments online 'going viral' to a far wider NHS, national or even international audience. Also, the current ease with which cyber abuse can take place anonymously, alerts us to be vigilant in the naming of abuse when and where we see it, and not be part of a burgeoning bystander crowd that is complicit in the abuse, as to 'like', 'forward' or remain silent about abusive content is to say 'yes' to the abuse taking place.

The NHS is committed via Guidelines such as these to ensure that staff can rest assured that we operate a policy of zero tolerance when it comes to cyber abuse. The NHS notes that identifying and addressing cyber abuse is not a curtailment of freedom of expression or speech, when we understand that our right to Freedom of Speech does not equate to a Freedom to Abuse.

The effective enactment of this position throughout the NHS sets the tone for a mutually respectful work environment that fosters trust in communication and inspires our staff to develop themselves and the quality of their service delivery throughout their career. But this can only be possible if staff to play their part in a commitment to being responsible at all points in their communication with and regarding others across all forms of digital and online communication, and just as the online world extends well beyond the workplace, this responsibility encompasses what and how you express about colleagues in and outside of work hours online.

Abuse Online or Offline is unacceptable – whether it is to colleagues, patients, the organisation, or the wider community.

This is particularly pertinent in an environment where safeguarding children, young people and adults at risk of harm or abuse is paramount.

The NHS has a duty of care towards all our staff under the Health and Safety Act 1974 and this document focuses on conduct in relation to all cyber communication as part of its care for its staff and directly resulting in supporting the care of its patients.

OUR COMMITMENT

NHS Organisations commit to the following:

- Adopt as a minimum standard this *Guidance on Cyber Abuse in the Workplace - NHS*, and produce local procedures from this NHS baseline.
- Ensure the Board Team and Senior Managers of the organisation are aware of cyber abuse, the potential risks in the organisation and that they have clear policies and procedures to support both staff and line managers.
- Nominate an independent and trustworthy point of contact for managers and staff in the organisation to raise a cyber abuse concern where needed.
- Brief Managers to enable them to recognise and handle cases of cyber abuse, providing them with the support of case studies (See Appendices).
- Include orientation on NHS guidance and standards in online and digital communication, and the responsibility of staff, at all new Staff Induction.
- Provide social media and electronic communications training for managers and staff which includes practicalities such as how to take screen shots and gather evidence, how to report cyber abuse to social media providers, how to spot cyber abuse, and how to support colleagues or staff if they are being cyber abused.
- Ensure HR teams are specifically aware of how to address cyber abuse issues and are equipped to support managers and teams when cyber abuse arises at work.
- Offer specific support to Social Media Teams, Communications Teams in the NHS in the event that staff experience cyber abuse from people outside of the NHS, including dealing with abuse such as defamatory, malicious or harassing, bullying comments on the organisational social media sites.
- Report cyber abuse incidents as part of monitoring cyber abuse activity and continuing to safe guard the organisation.
- Act to prevent re-posting on internal and external posting sites, through education on reporting mechanisms.
- Encourage networking with other organisations outside of the NHS about their experiences of cyber abuse, particularly with communications and social media teams.
- Work with and report to law enforcement where applicable.

TAKING ACTION AGAINST CYBER ABUSE

Cyber Abuse in Law

The Equality Act 2010 extends legal protection against harassment on the grounds of age, disability, gender reassignment, race (including colour, nationality and ethnic or national origins), religion or belief, sex and sexual orientation. The NHS will ensure compliance of the 2010 Act until subsumed by further legislation.

Whilst cyber abuse is not specifically defined in UK law at present, there are criminal laws that apply in terms of harassment or threatening and menacing communications:

- *Protection from Harassment Act 1997*
- *Communications Act 2003*
- *Malicious Communications Act 1988*
- *Public Order Act 1986*
- *Obscene Publications Act 1959*
- *Computer Misuse Act 1990*
- *Crime & Disorder Act 1998*
- *Defamation*

The NHS recognises that it has a legal responsibility to ensure that its employees are not subjected to abuse at work. However, the intention of this Guidance is to prevent and eradicate all digital forms of abusive and offensive behavior in a zero tolerance environment, whether or not such behaviour is unlawful or not, the behaviour is unacceptable in the NHS.

GUIDANCE FOR MANAGEMENT TEAMS

The most immediate action with a cyber abuse case is to investigate whether there is a case for cyber abuse or not. It is important at this stage to gather evidence, including screen shots, dates and times of any abusive electronic communication and HR teams, Communications and Social Media Teams and managers need to know what type of evidence to collect.

The Organisation's Information or Communications team is a place of support to assist line managers in responding to cyber abuse cases, by offering advice about the internet within the organisation, and how to deal with social media website or social network sites directly in relation to reporting abusive content, or getting abusive content taken down.

In cases of cyber abuse, and specifically defamation, local line managers may choose to seek legal advice, notify the organisation's Insurers and report the incident to the police as the cyber abuse incident may require further investigation and action outside of the organisation. Details of where

to find legal advice, how to contact the insurers, and the local police can be offered to managers as part of cyber abuse awareness raising.

NHS Organisation Policy Resources
Staff and managers may use one of the following organizational policies through which to raise a cyber abuse issue, particularly where cyber abuse is mentioned in the policy (and where cyber abuse is not specifically mentioned refer to bullying and harassment, or conduct at work, or dignity at work as well as the use of social media at work):

- Confidentiality – Code of Practice
- Internet Usage & Security Policy
- Data Protection Policy
- Crime and Disorder Act
- Information Security Policy
- Email Use Policy
- Email and Electronic Communications Policy
- Dignity and Respect Policy
- Bullying and Harassment Policy
- Disciplinary Policy and Procedure
- Confidentiality and Security Policy
- Information governance policy
- Information Risk Management policy
- Whistleblowing Policy
- Standards of Business Conduct Policy
- Media Policy
- Disclosure to the Police Policy
- Freedom of Information Policy
- Homeworking and Mobile Computing Equipment
- Safeguarding children, young people and vulnerable adults

In the end whichever policy is used, if there is a case to be investigated it will ultimately go through the Disciplinary Policy and Procedure. Where there have been cases of cyber abuse misconduct investigated in the NHS to date the majority of these have been investigated using the disciplinary procedure resulting in:

- Suspension during investigation
- Informal Counseling
- Social Media Training or other Electronic Communications Training
- Verbal warning
- First Written Warning
- Final Warning
- Dismissal

Where a department or team has had a cyber abuse investigation, line managers can where appropriate debrief the team, and ensure there are no outstanding issues once the cyber abuse investigation is complete. This may include emotional issues that still remain unresolved.

Safeguarding Cases

An important note here is that some cases of cyber abuse are also a safeguarding issue, as the NHS is a working environment where the protection of children, young people and vulnerable adults is paramount. During any investigation into cyber abuse, referring to safeguarding guidelines is an important step to take.

GUIDANCE FOR STAFF

The responsibility for a zero tolerance across all NHS workplace environments cannot solely rely on a written policy, training in cyber abuse, a management that is informed and delivering on appropriate action to address reports of cyber abuse. If we are to have zero tolerance of cyber abuse, as a team we must recognise we are all responsible for the quality of communication expressed in the organisation, with our service users and our contract providers.

What you can do:

- Report any potentially defamatory material to their line manager as soon as it is identified so that steps can be taken to investigate it and remove it permanently. If your allegation is against your Line Manager then speak to their manager or the HR department.
- If you feel you have been targeted on social media because of your role or because of a protected characteristic (your race, gender, disability, age, religion/belief or sexual orientation) or you feel you are being cyber bullied or cyber harassed, cyber stalked or cyber abused seek help and advice as soon as possible.
- The importance of evidence cannot be overemphasized, so it is important that you save a copy or take screenshots of the posts or messages, noting the time and date they were posted. Similarly, if being abused by phone log the time and date you received the phone calls.
- Report any cyber abuse activity directed towards you to the social media site owners, following their reporting procedures (e.g. Facebook, Twitter).
- Block abusive individuals from interacting with you on social media or other sites.
- Report cyber abuse to the Police where appropriate.
- If you have been affected by cyber abuse, seek support from an Employee Assistance Programme where counselling is offered or your Occupational Health Department can also offer you support.
- A point to note is that where the organisation's computer facilities are used to harass or abuse another, a record of this is likely to be found on the IT servers. And where there are postings online e.g. on a social media site the digital footprint is very difficult to erase.
- Where you suspect cyber abuse even if not directly related to you, if you are notified of or are concerned about an abusive or defamatory post, profile, comment or page relating to another employee or service, report it immediately to your line manager. The line manager should arrange for the post to be reviewed, and where appropriate, the post should be reported as abuse with the relevant site's existing reporting process via the engagement and communications team. A screenshot should be recorded of the comment. Be supportive of colleagues who may be subject to bullying and/or harassment.

- If cyber abuse has taken place using equipment that is not part of the your organisation it is much harder for the organisation to gather evidence. Internet service providers have Complaints Procedures that can be followed, but will generally only provide data to the police. However, it is still possible for your organisational Internet Services Department to take action to protect you, such as blocking emails from external email addresses or providing advice on how you could get an offensive posting on a social networking site removed.

MONITORING & REVIEW

The NHS has a duty of care towards staff and service users, and will take action, including disciplinary action if necessary, whether the abuse, harassment or bullying is taking place using workplace equipment or not.

Human Resources have the responsibility for monitoring all cyber-abuse cases through the audit process. Such data will inform future policy development and be made available under the Freedom of Information Act to ensure transparency and accountability and affect the development of national policies on cyber-abuse. The NHS acknowledges that the way in which we communicate continues to rapidly change, and thus aims to review this Guidance by 2018.