ONLINE SAFETY POLICY

THE PURPOSE OF THIS POLICY STATEMENT

Voices of Colour works with young people aged 15-25 as part of its activities. These include running a digital skills and leadership development programme online.

The purpose of this policy statement is to:
- ensure the safety and wellbeing of young people is paramount when adults and young people are using the internet, social media or mobile devices
- provide staff, facilitators and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, facilitators, volunteers, young people and anyone involved in Voices of Colour activities.

LEGAL FRAMEWORK

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect young people in England/Northern Ireland/Scotland/Wales. Summaries of the key legislation and guidance are available on:
- online abuse learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
- bullying learning.nspcc.org.uk/child-abuse-and-neglect/bullying
- child protection learning.nspcc.org.uk/child-protection-system

WE BELIEVE THAT:

- Young people should never experience abuse of any kind
- Young people should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

WE RECOGNISE THAT:

- The online world provides everyone with many opportunities; however it can also present risks and challenges
- We have a duty to ensure that all young people and adults involved in our organisation are protected from potential harm online
- We have a responsibility to help keep young people safe online, whether or not they are using Voices of Colour's network and devices
- All young people, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- Working in partnership with young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

WE WILL SEEK TO KEEP YOUNG PEOPLE SAFE BY:

- Appointing an online safety coordinator
- Providing clear and specific directions to staff, facilitators and volunteers on how to behave online through our behaviour code for adults
- Supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- Developing an online safety agreement for use with young people
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a young person
- Reviewing and updating the security of our information systems regularly
- Ensuring that user names, logins, email accounts and passwords are used effectively
- Ensuring personal information about the adults and young people who are involved in our organisation is held securely and shared only as appropriate
- Providing supervision, support and training for staff, facilitators and volunteers about online safety
- Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

IF ONLINE ABUSE OCCURS, WE WILL RESPOND TO IT BY:

- Having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- Providing support and training for all staff, facilitators and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

RELATED POLICIES & PROCEDURES

This policy statement should be read alongside our organisational policies and procedures, including:

- Child Protection Policy
- Safeguarding Policy
- Privacy Policy

VOLUNTEERS & CONTRACTORS

Key Responsibilities:

- Read, understand, sign and adhere to the online safety agreement
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

PARTICIPANTS

Key Responsibilities:

- Read, understand, sign and adhere to the online safety agreement
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk within the team if there are problems

EXTERNAL ORGANISATIONS

Key Responsibilities:

- Any external individual/organisation will read, understand, sign and adhere to the online safety agreement
- Support the organisation in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the staff, volunteers, contractors and participants

HANDLING DATA & INCIDENTS

It is vital that all staff and facilitators recognise that online-safety is a part of safeguarding. General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the session. Any concern/allegation about staff misuse is always referred directly to the Director, unless the concern is about the Director in which case the compliant is referred to the Board of Directors.

BULLYING

Online bullying should be treated like any other form of bullying and actions outlined within our child protection and safeguarding policy will be followed where necessary.

SEXUAL HARASSMENT AND VIOLENCE

- Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the organisations's full safeguarding guidance.
- Staff should work to foster a zero-tolerance culture. The guidance stresses that organisation's must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate.

DATA PROTECTION & DATA SECURITY

All participants, staff, facilitators, volunteers and contractors are bound by our data protection policy and agreements, which you can request a copy of which outlines our processes in place for the above.

ELECTRONIC COMMUNICATION

General principles for email use are as follows:

- Email is the primary means of electronic communication to be used between staff and participants
- We may set up alternative communication channels such as via Slack or WhatsApp, depending on what each cohort feel comfortable with using
- Appropriate behaviour is expected at all times, and these platforms should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the organisation into disrepute or compromise the professionalism of staff

---

FURTHER INFORMATION FOR PARENTS & CARERS FOR KEEPING YOUNG PEOPLE SAFE ONLINE

The following websites provide information for organisations and parents about online safety to help them protect their child from harm:

- NSPCC / O2 HELPLINE 0808 800 5002 – www.o2.co.uk/help/online-safety
- Child Exploitation and Online Protection Centre – www.ceop.police.uk/safety-centre
- Childnet – www.childnet.com
- The UK Safer Internet Centre – www.saferinternet.org.uk