Online Safety Policy

1. Introduction

We recognise that the online world provides many positive opportunities, however it can present risks and challenges to children and young people as well as staff and volunteers. We have a duty to ensure all children and young people in our organisation are safeguarded and protected from harm online. Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices as well as Artificial Intelligence (AI). This is not an exhaustive list.

Online Safety includes the use of photography and video, the internet and social media sites, mobile phones and smart watches. Our online safety policy is consistent with our wider safeguarding policy.

It is the overall responsibility of the Lead Safeguarding Officer (LSO) for ensuring the safety of all children, young people, and adults within the organisation when online as well as the conduct of Active Norfolk staff and volunteers. They will act as Online Safety Lead with support from the Marketing & Communications Lead Officer.

2. Platforms for Online Abuse and Types of Abuse

Online abuse can happen anywhere online that allows digital communication, such as: social networks, text messages and messaging apps, email and private messaging, online chats, online gaming, and live streaming sites. Staff, volunteers and children may experience several types of abuse online:

- Bullying/cyberbullying
- Emotional abuse-which can include emotional blackmail.
- Sexting-pressure or coercion to create sexual images.
- Sexual abuse
- Sexual exploitation
- Grooming-perpetrators may use online platforms to build a trusting relationship with the child to abuse them.

3. National Guidance and Legislation on Online Safety

a. The Online Safety Act 2023

The Act makes companies that operate a wide range of popular online services legally responsible for keeping people, especially children, safe online. Services must do this by assessing and managing safety risks arising from content and conduct on their sites and apps.

The Law is based on 3 fundamental duties:

- protecting children.
- shielding the public from illegal content.
- and helping adult users avoid harmful – but not illegal – content on the biggest platforms.

4. Protecting Children

There are 2 categories of harmful content to children that tech firms must deal with.

- The first is “primary priority content,” such as pornography and the promotion of suicide and eating disorders (below the threshold of criminality). If sites allow such content, children must be prevented from encountering it and the Act expects age-checking measures to be used for this.
- The second is “priority content” such as bullying and posts that encourage children to take part in dangerous stunts or challenges. Children in age groups judged to be at harm from such content– must be protected from encountering this kind of material.

For the latest updates on The Online Safety Act implementation, we will consult the guidance from Ofcom: https://www.ofcom.org.uk/online-safety

b. The Data Protection Act 2018

To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. This legislation also applies to all electronic and online data. Active Norfolk abides by all aspects of Norfolk County Council policy in this area.

5. Responding to online abuse and how to report it at Active Norfolk

The Lead Safeguarding Officer (LSO) or Designated Safeguarding Lead (DSO) should be used as a first point of contact for concerns and queries on online abuse. All concerns about a child should be reported to them without delay and recorded in writing using the agreed system as set out in the safeguarding policy.

Following receipt of any information raising concern about online abuse, the LSO will consider what action to take and seek advice from Active Norfolk's Sport Welfare Officer (SWO), Norfolk Children's Advice & Duty Service (CADS) as required.

If, at any point, there is a risk of immediate serious harm to a child, The Children's Advice and Duty Service (CADS) should be contacted. Anybody can contact CADS in these circumstances.

Depending on the type of online abuse concerned, this will also be reported using the relevant method below:

Criminal Sexual Content-If the concern is about online criminal sexual content, this will be report to the Internet Watch Foundation here.

Child Exploitation and Online Protection- If the concern is about online sexual abuse and grooming, a report should also be made to the Child Exploitation and Online Protection (CEOP)

Report Remove Tool-Young people under 18 will be supported to use the Report Remove tool from Childline to confidentially report sexual images and videos of themselves and ask these to be removed from the internet. This can be reported here.

Online Terrorism or Extremism Content-If online material is found which promotes terrorism or extremism this will be reported to ACT Action Against Terrorism. A report can be made online here.

Online Hate Content-If online content incites hatred this will be reported online to True Vision here.

6. Sources of support on Online Safety

UK Safer Internet Centre-For free, independent, expert advice on dealing with internet safety problems contact the Helpline. Professionals Online Safety Helpline-0344 3814772 or helpline@saferinternet.org.uk

Childnet For online safety information and advice for professionals working with children and young people. 020 7639 6967 info@childnet.com

Internet Matters Supports parents and professionals with resources and guidance on child internet safety.

7. We have the following measures to promote online safety:

- A firewall and robust antivirus software via Norfolk County Council (NCC)
- Access to the internet is via a secure work network platform and severs all provided by (NCC). More information here: Home - Intranet - Norfolk County Council
- An encrypted and password protected Wi-Fi network.
- Norfolk County Council MyIT filters any inappropriate websites or content based on inappropriate search terms.
- No removable media containing personal or sensitive data (e.g. USB sticks or devices that leave our organisation) are used by Active Norfolk staff.
- Personal data is managed in in compliance with **The Data Protection Act 2018**
- The latest operating system security updates installed
- Passcode and lock screened are used on all devices.
- Staff and volunteers are not permitted to use any devices in the organisation for personal use.

- Any photography must be done using Bring Your Own Device, using Microsoft Teams direct to the marketing team.
- Online safety information and awareness is provided to website users to increase awareness of online safety and promoting online safety events e.g. Safer Internet Day.

8. Our organisation uses a range of online services to communicate which include:

- Website
- Social media pages
- Social media messaging
- Online portal pages
- Closed messaging systems
- Email

All communications take place through clear and established systems and will be professional in nature.

- All staff/volunteers will be asked to read and sign the Safety Online Agreement which sets out rules on the use of personal online communications.
- Our organisation uses digital images and video as a tool to record and inform stakeholders, partners, families and parents of activities.
- Staff may only use a personal device if they have installed **Bring Your Own Device**, supplied downloaded via Norfolk County Council MyIT. All videos and images must be taken via Microsoft Teams only and sent direct to the marketing department.
- The Marketing Department will provide a professional photographer for any other digital images or video.
- We gain written permission from parents to record and use digital images and video of their children. Through this process, we respect their rights under the Data Protection Act 2018.
- Our organisation stores images securely by using Norfolk County Council platforms and we meet legal requirements on how long we retain those images. Parents/carers are asked to sign a declaration which sets out how they are to use to digital images/videos of their child taken by them at the organisation.
- There are safeguarding risks associated with the use of personal mobile phones and smart watches. It is the responsibility of all members of staff to be vigilant and to report any concerns.

9. Rules on Personal Mobile Phones:

Personal mobile phones must have Bring Your Own Device installed via the Norfolk County Council MyIT.

10. Rules on Smart Watches

Only smart watches without cameras are permitted to be worn purely to perform the function of a watch when working with children.

a. The following steps must be adhered to by staff wearing smart watches without cameras:

- During activities which involve children or adults at risk, all other functions must be disabled with Bluetooth disconnected or on ‘flight mode,’ this will ensure there is no internet connection or Wi-Fi connection.
- Smart watches are not allowed to connect to the organisations Wi-Fi at any time.
- The watch must always be on silent, during activities involving children or adults at risk.
- Staff should not use their smart watch to access photos or images while working with children or adults at risk.
- With ongoing technology advances, the organisation reserves the rights to request the removal of a Smart Watch if it deemed a safeguarding risk to children or adults at risk.

11. The Online Safety Lead will:

- ensure all staff/volunteers have current awareness of the online safety policy and incident reporting procedures.

- take daily responsibility for any online safety issues and play a leading role in establishing and reviewing the online safety policies/procedures with support from the Safeguarding Continuous Improvement Group.
- offers advice and support to staff and volunteers.
- completes training on online safety.
- keeps up to date with developments in online safety and cascades these to staff/volunteers.
- understands and knows where to obtain additional support and where to report online safety issues.
- receives reports of online safety incidents and keeps a log of incidents to inform future online safety developments.
- communicates with parents/carers about online safety.
- monitors online incident logs.

12. Staff and volunteers are responsible for ensuring that:

- they have an awareness of this online safety policy and fully adhere to all associated procedures.
- they have read, understood, and signed the staff/volunteer acceptable use agreement and will fully follow the standards set out within it.
- follow the procedures for reporting and recording online safety issues.
- demonstrate positive online behaviours.

Revision date	Reviewed by	Board approval	Date of Board approval
9th August 2024	A Roberts / CIG	Actioned	11th Sept 2024

<u>Online Acceptable Use for Staff and Volunteers</u> (on forms)

This Acceptable Use Agreement is intended to ensure that:

- staff and volunteers will act responsibly to stay safer while online, being a good role model.
- effective systems are in place for the online safety of all users and the security of data.

- staff and volunteers are aware of, and can protect themselves from, potential risks in their use of online technologies.

For my professional and personal safety, I understand that:

- I will ensure that my online behaviours will be professional, both to protect myself and the organisation.
- When communicating professionally I will only use the technology provided by the organisation.
- I will not use my own personal devices, personal email addresses, personal social networking accounts to conduct any work for the organisation.
- I will not use the organisation’s technology for personal use.
- I will follow the rules for personal mobile phone usage and personal smart watch usage as set out in the safeguarding policy and online safety policy.

For the safety of others:

- I will only access materials and content that are legal and appropriate.
- I will only use ‘Bring Your Own Device’ approved devices to record images of children in appropriate circumstances for work purposes.
- I understand reporting procedures and will immediately report any illegal, harmful, or inappropriate incident.
- When using social media, I will ensure it does not negatively impact on the organization's reputation or the safeguarding of its members.
- Any personal data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by the organization's policy to disclose such information to an appropriate authority.
- I will only download content that I have the right to use.
- I will only use my personal device/technology within the organisation if I have permission and use it within the agreed rules.
- I understand that any images I publish will be with the owner’s permission and follow the organisation’s policy.
- I will only install programmes on the systems devices belonging to the group, with permission.