We recognise that the online world provides many positive opportunities, however it can present risks and challenges to children and young people. 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.

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 DSL for ensuring the safety of all children, young people, and adults within the organisation when online.

The Online Safety Lead or DSP/SLP will:

- ensures all staff/volunteers have current awareness of this online safety policy and incident reporting procedures.
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies/procedures.
- 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

Staff and volunteers are responsible for ensuring that:

- they have an awareness of the online safety policy and 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.

- educate children and young people on how to stay safe online.

- demonstrate positive online behaviours to children.

Staff and volunteers will be given the Online Acceptable Use Agreement to sign during their induction. The Agreements set out the standards which need to be adhered to when being online.

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. 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.

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.

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.

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.

We have the follow measures in place to promote online safety:

- A firewall and robust antivirus software
- A recognised internet service provider - EE
- Our internet service provider offers the following filtering and monitoring service
- An encrypted and password protected Wi-Fi network
- The Online Safety Person or DSP monitors and filters any inappropriate websites
- We have added the **'Report Harmful Content'** Button to our website so that users can easily report harmful content
- Children are always supervised by a staff member or volunteer when using devices online
- Access to online content in the organisation is through using the child friendly search engine **SWGL Swiggle**
- Any removable media containing personal or sensitive data (e.g. USB sticks or devices that leave our organisation) are secured through password and/or encryption
- Personal data is managed in in compliance with The Data Protection Act 2018
- Having the latest operating system security updates installed
- Children are not permitted to bring in their own devices from home
- Passcode and lock screened are used on all devices
- If children are using devices and do not need online access, this is turned off before they are given the device
- Staff and volunteers are not permitted to use any devices in the organisation for personal use
- Signed Parental permission is gained if children are able to go online in the organisation
- Promoting online safety awareness to the children we work with by:
  - having informal conversations where we discuss online safety
  -children will be supported to recognise not everything on the internet is true or accurate
  - staff/volunteers will act as good role models in their use of online technologies.
  -rules for the use of devices will be posted in areas where these devices are in use
  -we have a code of conduct for children which sets out how they are expected to behave while online in our organisation

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

- *Website*
- *Social media pages*
- *Social media messaging*
- *Text messaging*

- *Email*

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

Communications are monitored for concerns/complaints. There are processes in place to respond and resolve complaints or comments concerning our organisation or staff/volunteers.

All staff/volunteers will be asked to read and sign the Online Acceptable Use 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 families and parents of the progress and activities of their children. The devices we use for recording images of children are provided by the organisation for staff/volunteers to use professionally.

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 locked and secured online storage, and we meet legal requirements on how long we retain those images.

Parents are asked to sign a declaration which sets out how they are to use 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. Our organisation has measures in place to protect children from the unacceptable use of technology or exposure to inappropriate materials on this technology. It is the responsibility of all members of staff to be vigilant and to report any concerns.

Rules on Personal Mobile Phones

-Personal mobile phones are to be stored securely in bags/cars.

-Personal mobile phones are only to be used in emergencies

-Personal mobile phones are always to be stored on silent mode

-Personal mobile phones are not to be used to conduct any work for the organisation

-Personal mobile phones are not allowed to connect to the Wi-Fi at any time

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.

The following steps must be adhered to by staff wearing smart watches without cameras:
-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 be on silent at all times
-Staff should not use their smart watch to access photos or images while working
-Staff need to be vigilant of others checking their smart watches and remind them of our policy
-With ongoing technology advances, the organisation reserves the right to request the removal of a Smart Watch if it is deemed a safeguarding risk to children.

The *DSP* 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 DSP will consider what action to take and seek advice from the Norfolk Children's Advice & Duty Service (CADS) as required.

If we feel a child is at risk of immediate harm, we will call the Police immediately on 999.

If we are concerned that a child or children is experiencing or likely to suffer significant harm, we will telephone (CADS) immediately on 0344 800 8021. 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 reported 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.

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.

Name: Sam Boon

Signed: 

Date: 20/05/2026

Date for review: 20/05/2027

Online Acceptable Use Agreement for Staff and Volunteers

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.
- 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 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 the organisation'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 organisation'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 use the organisation's equipment to record images of children.
- I will protect my online personal information to prevent access to children and families. This will be done by not accepting friend requests from any parent or child. I will keep my social media account settings private and not display where I work.
- I will inform the appropriate person if I find any damage or faults with technology.
- I will only install programmes on the systems devices belonging to the group, with permission.

If the organisation suspects, or becomes aware, that a staff member/volunteer has breached this Online Acceptable Use Agreement the organisation will address this in accordance with the Disciplinary Policy.

Name: Sam Boon

Signed: 

Date: 20/05/2026

Online Acceptable Use Agreement for Children and Young People

This is how we stay safe when we go online in the organisation:

- I will ask a staff member or volunteer if I want to use a device to go online.
- I will only do activities online that a staff member or volunteer has told me that I can use.

- I will take care of the computers, tablets, and other equipment.
- I will ask for help from a staff member or volunteer if I am not sure what to do or if I think I have done something wrong.
- I will tell a staff member or volunteer if I see something that upsets me on my screen or someone else's.
- If I see that another child is doing something wrong online, I will tell a staff member or volunteer.
- I know that if I break the rules I might not be allowed to go online again.

Signed (parent): ……

Date: ……

<u>Parental Consent Form for Online Usage for Their Child</u>

A copy of the Children's Acceptable Use Agreement is attached to this permission form, so that parents are aware of the organisation's expectations of the children in our care.

As the parent, I give permission for my child to use the organisation's technology and devices.

I know that the organisation has made my child aware of the *Acceptable Use Agreement.*

I understand that the organisation will take reasonable precautions to ensure that my child will be safe when online, however, I understand that whilst this manages risk, it cannot eliminate it.

I understand that my child's online activity will be supervised and monitored, and that the organisation will contact me if they have concerns about any possible breaches of the Online Acceptable Use Agreement.

I understand that the organisation will take appropriate action in the event of any incidents.

I will encourage my child to adopt safe use of online technologies.

Parent/Carers Name: ……

Name of Child: ……

Signature: ……

Date: ……

Parental Consent form for the Use of Digital Images and Videos

The use of digital/video images plays an important part in our activities. Children, staff and volunteers may use the organisation's devices to record images/videos of those activities. These images/videos will be used through publication in our printed materials, our website and on social media pages.

The organisation complies with the Data Protection Act and requests parental permission before taking images and videos of children. Names are not published alongside images.

As the parent of the below child, I agree to the organisation taking and using digital images/videos of my child. I understand the images and videos will only be used to support legitimate activities or in publicity that promotes the work of the organisation.

Parent/Carers Name:

Signature:

Name of Child:

Date:

I agree that if I photograph or film my child at the organisation, I will adhere to the following:

- Images and videos will be for my own or family's personal use only.
- I will not photo or record any other child without permission from that child's parent.
- If I share images/videos online which feature other children, I will only do so with permission from the parent.
- If I share images and videos on social media taken in the organisation, I will ensure the post is not set to public.
- If I am unsure whether I can share photos and videos I will speak to the DSP

Parent/Carers Name:

Signature

Date: