



## Online Safety Policy

<b>Policy Headings</b>	<b>Elite Studio (EA) Ltd</b>
<i>Introduction</i>	<p>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. Our online safety policy is consistent with our wider safeguarding policy.</p> <p>It is the overall responsibility of our online safeguard lead for ensuring the safety of all children, young people, and adults within the organisation when online.</p>
<i>The Role of the Online Safety Lead</i>	<p><u>The Online Safety Lead or DSP/SLP is: Danielle Crofts</u></p> <ul style="list-style-type: none"> <li>• <u>ensures all staff/volunteers have current awareness of the online safety policy and incident reporting procedures.</u></li> <li>• <u>takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies/procedures.</u></li> <li>• <u>offers advice and support to staff and volunteers.</u></li> <li>• <u>completes training on online safety.</u></li> <li>• <u>keeps up to date with developments in online safety and cascades these to staff/volunteers.</u></li> <li>• <u>understands and knows where to obtain additional support and where to report online safety issues.</u></li> <li>• <u>receives reports of online safety incidents and keeps a log of incidents to inform future online safety developments.</u></li> <li>• <u>communicates with parents/carers about online safety.</u></li> <li>• <u>monitors online incident logs</u></li> </ul>
<i>Staff / Volunteers Responsibilities</i>	<p><u>Staff and volunteers are responsible for ensuring that:</u></p> <ul style="list-style-type: none"> <li>• <u>they have an awareness of the online safety policy and procedures.</u></li> <li>• <u>they have read, understood, and signed the staff/volunteer acceptable use agreement and will fully follow the standards set out within it.</u></li> <li>• <u>follow the procedures for reporting and recording online safety issues.</u></li> <li>• <u>educate children and young people on how to stay safe online.</u></li> <li>• <u>demonstrate positive online behaviours to children.</u></li> </ul>
<i>Acceptable Online Usage for Staff and Volunteers</i>	<p>Staff and volunteers will be given the Online Acceptable Use Agreement to sign during their induction. The Agreements sets out the standards which need to be adhered to when being online.</p>
<i>Platforms for Online Abuse and Types of Abuse</i>	<p>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:</p> <ul style="list-style-type: none"> <li>• <u>Bullying/cyberbullying</u></li> <li>• <u>Emotional abuse</u>-which can include emotional blackmail</li> </ul>

- 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.

Ofcom have said that the new laws will roll out in three phases as follows, with the timing driven by the requirements of the Act and relevant secondary legislation: Phase one: Illegal content, Phase two: Child safety, pornography, and protecting women and girls, Phase three: Additional duties for categorised services. For the latest updates on The Online Safety Act implementation we will consult the guidance from Ofcom: <https://www.ofcom.org.uk/online-safety>

**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.

**Keeping Children Safe in Education 2023** (this outlines the responsibilities that schools and colleges have in safeguarding children, including a requirement to

*National Guidance and Legislation on Online Safety*

	<p>ensure appropriate levels of online filtering and monitoring are in place-refer to pages 35-38).</p> <p><b>Do the filtering and monitoring requirements apply to children in settings other than schools as part of their e-safety responsibilities?</b> The Safer Internet Centre encourages other organisations who work with children and provide technology and online access, to adopt the same standards highlighted within Keeping Children Safe in Education 2023.</p>
<p><i>Measures we have in our organisation to promote online safety.</i></p>	<p>We have the follow measures in place to promote online safety:</p> <ul style="list-style-type: none"> <li>● A firewall and robust antivirus software</li> <li>● A recognised internet service provider-BT</li> <li>● Our internet service provider offers the following filtering and monitoring service BT Virus Protect, BT Web Protect and BT Parental Controls.</li> <li>● An encrypted and password protected Wi-Fi network</li> <li>● The Online Safety Person or DSP monitors and filters any inappropriate websites or content in the following ways <b><u>SWGL Test Filtering Site</u></b></li> <li>● We have added the '<b><u>Report Harmful Content</u></b>' Button to our website so that users can easily report harmful content</li> <li>● Children are always supervised by a staff member or volunteer when using devices online</li> <li>● Access to online content in the organisation is through using the child friendly search engine <b><u>SWGL Swiggle</u></b></li> <li>● 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</li> <li>● Personal data is managed in in compliance with The Data Protection Act 2018</li> <li>● Having the latest operating system security updates installed</li> <li>● Children are not permitted to bring in their own devices from home</li> <li>● Passcode and lock screened are used on all devices</li> <li>● If children are using devices and do not need online access, this is turned off before they are given the device</li> <li>● Staff and volunteers are not permitted to use any devices in the organisation for personal use</li> <li>● Signed Parental permission is gained if children are able to go online in the organisation</li> <li>● Promoting online safety awareness to the children we work with by: <ul style="list-style-type: none"> <li>- <u>having informal conversations where we discuss online safety</u></li> <li>- <u>children will be supported to recognise not everything on the internet is true or accurate</u></li> <li>- <u>staff/volunteers will act as good role models in their use of online technologies.</u></li> <li>- <u>rules for the use of devices will be posted in areas where these devices are in use</u></li> <li>- <u>we have a code of conduct for children which sets out how they are expected to behave while online in our organisation</u></li> </ul> </li> <li>● Online safety information and awareness is provided to parents to increase their awareness of online safety risks and issues to children at home. This is</li> </ul>

	<p>done through:</p> <p><i>-letters, newsletters, website.</i></p> <p><i><u>-meetings with parents</u></i></p> <p><i><u>-providing links to relevant good practice information/websites</u></i></p>
Online Communications	<p>Our organisation uses a range of online services to communicate which include:</p> <ul style="list-style-type: none"> <li>● Website</li> <li>● Social media pages</li> <li>● Social media messaging</li> <li>● Text messaging</li> <li>● Online portal pages</li> <li>● Closed messaging systems</li> <li>● Email</li> </ul> <p>All communications take place through clear and established systems and will be professional in nature.</p> <p>Communications are monitored for concerns/complaints. There are processes in place to respond and resolve complaints or comments concerning our organisation or staff/volunteers.</p> <p>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.</p>
Digital Images and Videos	<p>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.</p> <p>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.</p> <p><u>Our organisation premises also uses CCTV to protect all those who attend. We ensure these systems meet statutory and safeguarding requirements and the data recorded by these systems is compliant with the Data Protection Act 2018. There is clear signage indicating that CCTV is in use.</u></p> <p><u>Our organisation stores images securely with password protected devices and we meet legal requirements on how long we retain those images.</u></p> <p><u>We share images with parents through secure routes that include: Our online Social media which is password protected.</u></p> <p><u>Parent's 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</u></p>
	<p>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.</p>

<p><i>Personal Mobile Phones and Smart Watches</i></p> <p><b>It is down to each organisation to decide what their rules are on the use of mobile phones and smart watches. However, you must show in your safeguarding policy and online safety policy how you mitigate risks with these devices.</b></p>	<p><b>Rules on Personal Mobile Phones</b></p> <ul style="list-style-type: none"> <li>-Personal mobile phones are to be stored securely in a locker</li> <li>-Personal mobile phones are only to be used in the following area staff only area's</li> <li>-Personal mobile phones are always to be stored on silent mode</li> <li>-Personal mobile phones are not to be used to conduct any work for the organisation</li> <li>-Personal mobile phones are not allowed to connect to the Wi-Fi at any time</li> </ul> <p><b>Rules on Smart Watches</b></p> <p>Watches with cameras will need to be removed before work and stored securely in Staff Lockers.</p> <p>Only smart watches without cameras are permitted to be worn purely to perform the function of a watch when working with children.</p> <p>The following steps must be adhered to by staff wearing smart watches without cameras:</p> <ul style="list-style-type: none"> <li>-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</li> <li>-Smart watches are not allowed to connect to the organisations Wi-Fi at any time</li> <li>-The watch must be on silent at all times</li> <li>-Staff should not use their smart watch to access photos or images while working</li> <li>-Staff need to be vigilant of others checking their smart watches and remind them of our policy</li> <li>-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</li> </ul>
	<p>The <i>Online Safety Lead</i> 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.</p> <p>Following receipt of any information raising concern about online abuse, the Online Safety Lead will consider what action to take and seek advice from the Norfolk Children's Advice &amp; Duty Service (CADS) as required.</p> <p>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.</p> <p>Depending on the type of online abuse concerned, this will also be reported using the relevant method below:</p>

<p><i>Responding to online abuse and how to report it</i></p>	<p><b><i>Criminal Sexual Content</i></b>-If the concern is about online criminal sexual content, this will be report to the Internet Watch Foundation <a href="#"><u>here</u></a>.</p> <p><b><i>Child Exploitation and Online Protection</i></b>- If the concern is about online sexual abuse and grooming, a report should also be made to the <a href="#"><u>Child Exploitation and Online Protection (CEOP)</u></a></p> <p><b><i>Report Remove Tool</i></b>-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 <a href="#"><u>here</u></a>.</p> <p><b><i>Online Terrorism or Extremism Content</i></b>-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 <a href="#"><u>here</u></a>.</p> <p><b><i>Online Hate Content</i></b>-If online content incites hatred this will be reported online to True Vision <a href="#"><u>here</u></a>.</p>
<p><i>Sources of support on Online Safety</i></p>	<p><b><u>UK Safer Internet Centre</u></b>-For free, independent, expert advice on dealing with internet safety problems contact the Helpline. Professionals Online Safety Helpline-0344 3814772 or <a href="mailto:helpline@saferinternet.org.uk"><u>helpline@saferinternet.org.uk</u></a></p> <p><b><u>Childnet</u></b> For online safety information and advice for professionals working with children and young people. <a href="tel:02076396967"><u>020 7639 6967</u></a> <a href="mailto:info@childnet.com"><u>info@childnet.com</u></a></p> <p><b><u>Internet Matters</u></b> Supports parents and professionals with resources and guidance on child internet safety.</p>
<p>Name: Keri Wooden</p> <p>Signed: Keri</p> <p>Manager Name: Hannah Gilson</p> <p>Date: 12/09/2025</p> <p>Date for review: 11/09/2025</p>	

## **Online Acceptable Use Agreement for Staff and Volunteers**

You will need to amend and add to this agreement depending on what the rules are in your organisation. Each organisation operates differently so what is appropriate for one, might not be practical for another.

### **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 (state what these are).
- 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 on 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. (Adapt this according to what the rules are in your organisation).
- 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:

Signed:

Date: .....

### **Acceptable Use Agreement for Children and Young People**

You will need to amend and add to this agreement depending on what the rules are in your organisation.

Each organisation operates differently and works with different ages of children, so what is appropriate for one, might not be appropriate for another.

Depending on the age of the children in your organisation, you might get them to create the agreement with you.

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 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: .....

Signed (child) .....

Date: .....

Depending on the age of the child and their level of understanding you might also choose to get them to sign this acceptable use agreement.

### **Parental Consent Form for Online Usage for Their Child**

A copy of the Children's Acceptable Use Policy 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 safer 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 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. ([delete/amend as appropriate](#)). Our organisation also uses CCTV to protect our community. We ensure that these systems meet statutory and safeguarding requirements and the data recorded is compliant with the Data Protection Act 2018. There is signage indicating CCTV is in use. ([delete/amend as appropriate](#)).

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. ([delete/amend as appropriate](#)).

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 ..... ([decide who this will be in your organisation](#))

Parent/Carers Name:

Signature

Date: