



Online Safety Policy

Policy Statement and Scope

Shine recognises that the online environment provides many positive opportunities, but it can also present risks and challenges to children and young people, Trustees, staff, volunteers and students where applicable. We have a duty to ensure everybody in our organisation is safeguarded and protected from harm online.

Online abuse is any type of abuse that happens through the internet, is facilitated through technology including computers, tablets, mobile phones and other devices that can access the internet. Our online safety policy is to run alongside our Safeguarding policy.

It is the overall responsibility of the Senior Manager and Designated Safeguarding Lead (DSL) Practitioners to ensure the safety of all children, young people and adults within the provision.

Roles and responsibilities of the DSL as the Online Safety Lead:

- Ensure all staff, Trustees, volunteers, and students where applicable will have awareness of the current online safety policy and incident reporting procedures
- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the policy and procedures.
- Will offer advice and support to staff and volunteers
- Complete online safety training and refresh as and when appropriate
- Keep up to date with developments in online safety and cascade these to all staff, Trustees, and volunteers
- Understand where to obtain additional support and where to report online safety issues
- Receive reports of and keep an up-to-date log of any online safety issues, and monitor incidence logs regularly
- Communicate with parents/carers about online safety

Responsibilities of staff and volunteers:

- 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.

Online 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. 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
- Criminal exploitation

Grooming-perpetrators may use online platforms to build a trusting relationship with the child to abuse them.

Guidance and Legislation:

The Online Safety Act 2023 is a new set of laws to protect children and adults online. The aim of this Act is to make the UK the safest place to be online by:

- Making it more difficult for young people to access harmful content online;
- Imposing new legal responsibilities on companies that provide online services, such as social media sites and search engines;
- Providing adults with greater choice over the content they see when using social media

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 ensure appropriate levels of online filtering and monitoring are in place-refer to pages 35-38).

Online Safety at Shine:

At Shine, our internet service provider (Osiris) manages our devices. Together we ensure we have firewalls and robust antivirus software on all electronic devices owned by Shine, and Osiris ensures regular updates of Shine's operating security systems.

We do not often permit the use of online devices for children and young people attending the provision. On occasions where the use of iPad's is permitted for leisure activity, Osiris have ensured that children and young people are only able to access the applications downloaded by their service onto the device. Shine has separate iPads for staff use. All iPads are password protected and do not allow any individual to download applications, or to access websites that use online communications; in addition to this wherever there are child-friendly versions of applications (for example, YouTube and search engines) these have been



installed. Osiris also oversee the use of computers which have the same firewalls and antivirus software. Children and young people will always be supervised by an adult while accessing online materials.

Osiris will flag any concerns raised by online use to the Senior Manager and support with appropriate next steps should this occur. The Senior Manager or DSLs will monitor for any access gained to inappropriate websites or content and will ensure they contact Osiris to get these added to their blocked or restricted sites as required.

Shine provides Wi-Fi which is password protected. This password will not be shared with persons unknown to Shine in any scenario. Staff, Trustees, volunteers and students where applicable will have access to the password where the Senior Manager or member of the Senior Leadership Team has assessed any risks.

Personal data stored on electronic devices, and any removable media containing personal or sensitive data (e.g. laptops that may leave our premises) are secured through password protection, and personalised access to folders tailored appropriately to the role of the individual. All personal data is managed in compliance with The Data Protection Act 2018 and with Shine's GDPR policy and procedures.

Online safety information and awareness is provided to parents through letters, newsletters and meetings. We are also able to signpost to relevant good practice information services and websites, and promote awareness through engaging with online safety events, e.g. Safer Internet Day. For children and young people who raise concerns about their use of online technologies, the Senior Manager or DSL will be informed and a meeting will take place to support their use at home. If a major concern arises staff will follow appropriate safeguarding procedures outlined in Shine's safeguarding policy.

Mobile phones and smart watches

All staff, Trustees, volunteers, visitors, students where applicable, children and young people are not permitted to bring their personal mobile phones or smart watches into the main play areas of Shine. Staff will leave their mobile phones and smart watches in the staff room on arrival. If staff are waiting for a phone call, they can leave their phone in the main office with the office staff who will call through and ensure there is enough cover for the individual to take the phone call outside of the main play areas.



Visitors, such as external professionals and parents/carers, and children and young people who do bring in a mobile phone and/or smart watch, will be asked to leave mobile phones and/or smart watches in the designated devices box on arrival.

Supporting children and young people with online safety

Wherever appropriate for the ability and understanding of children and young people accessing Shine's provisions staff will promote online safety awareness through informal conversations, particularly focussing on how not everything on the internet is true or accurate, and how we can recognise this. All staff, Trustees, visitors and students where applicable will act as good role models in their use of electronic devices and online technologies.

Online Communications:

Shine uses a range of online services to communicate which include: Tapestry, social media (Facebook and Facebook Messenger), text messaging, closed messaging systems (WhatsApp), website and emails.

All communications from Shine take place through clear and established systems and will be professional in nature. Shine will monitor communications consistently, especially for compliments, concerns and complaints. We have rigid processes in place to respond and resolve these, and a detailed complaints policy is in place should this occur.

Digital Images, Videos and Recordings:

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, and on occasion to support multiagency planning and reviews, and report back to Norfolk County Council Short Breaks Team. The devices we use for recording images of children are provided by the organisation for staff/volunteers to use and remain within Shine's premises. These are double locked in the main office. Any photos of children and young people will be retained in line with Shine's GDPR policy.

We gain written permission from parents to record and use digital images and video of their children whilst attending sessions at Shine, in line with the Data Protection Act 2018. For Nursery children, images may be shared with parent/carers through their Tapestry account, where a consent form has previously been signed for this use. Shine may wish to use photos of children and young people on their social media page and website; on these occasions staff will check that permission has been given in their registration documents, and ensure a courtesy call has been made to double check that parent/carers are happy for this use. Confirmation that consent remains the same will be sought on an annual basis. For any child



classed as a 'Looked After Child' (LAC), any photos taken will be limited to use in achievement books and shared with immediate carers only.

Shine uses CCTV to protect all those who attend the provision. These systems meet statutory and safeguarding requirements, and the data recorded by these systems is compliant with the Data Protection Act 2018. The CCTV system is serviced and regulated by The Alarm Co. There is clear signage indicating that CCTV is in use.

Reporting and Responding to Online Abuse:

The Senior Manager or DSL will be the first point of contact for concerns and queries about online use and abuse. All concerns about an individual should be reported immediately and recorded using the CPOMS system, or the 'safeguarding record of concern' or 'welfare record of concern' forms found in the filing cabinet in the staff room, in the 'leaders' folder and in the main office.

For any concern that has been raised the Senior Manager or DSL will consider what action to take and seek advice from the Norfolk Children's Advice and Duty Service (CADS) as required. In the case that there is risk of immediate serious harm to a child a referral should be made to CADS immediately – any individual can make a referral in these circumstances following the flowchart that is visible in the staff room.

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](#).



Other useful sources for 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.

Policy Review

Shine will review this policy annually and make changes to our policy and procedures in line with Norfolk Safeguarding Children Partnership's guidance and other current legislation.

Name: Rhiannon Jones/Senior Manager

Signed: Rhiannon Jones

Agreed by Trustees: 20th May 2024

Reviewed: 1st April 2026

Next review: April 2027

Reviewed by: Rhiannon Jones/Senior Manager