Online Safety Policy

Statement of intent

We recognise that the online world provides many positive opportunities, however it can present risks and challenges to children. We have a duty of care to ensure all children in our setting are safeguarded and protected from harm online. Although much of the newly published Online Safety Act (2023) is aimed at older children, we must never forget we are the gatekeepers of our young children's online presence. It is never too early to teach children about internet safety and for us, as their protectors, to ensure they grow up understanding how to keep safe while using this amazing tool.

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.

Our internet service provider is **BT**. This service is monitored by our IT services company **Beacon IT**.

Our Online Safety Leads are:

★ Wroxham Road: **Becky Potter**	**01603 787353**
★ Constitution Hill: **Beth Haywood**	**01603 427112**
★ White House Farm: **Alex Wells**	**01603 415821**

In their absence, the following member(s) of staff will deputise:

★ Wroxham Road: **Georgia Bellamy or Lucy Saunders**	**01603 787353**
★ Constitution Hill: **Jodie Harvey or Adele Reid**	**01603 427112**
★ White House Farm: **Daisy Drewery or Anna Terrington**	**01603 415821**

They can be contacted during nursery hours Monday - Friday (8am - 6pm).

The role of the Online Safety Lead

★ Ensures all staff/students have current awareness of the 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/students.
★ 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.

National guidance and legislation on online safety

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. Companies must do this by assessing and managing safety risks arising from content and conduct on their websites and applications. The law is based on three 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 two categories of harmful content to children that tech firms must deal with.

1. 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.

2. 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.

- ★ Phase one: Illegal content.
- ★ Phase two: Child safety, pornography, and protecting women and girls.
- ★ Phase three: Additional duties for categorised services.

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.

Aims

Digital Images and Videos

Once upon a time uses digital images and video as a tool to record and inform families of the progress and activities of their children. The devices we use for recording images of children are provided by us 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.
- ★ We store images securely by using password protected computers and tablets. and we meet legal requirements on how long we retain those images.
- ★ We share images with parents through their secure personal Tapestry account.
- ★ Parents 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.

Personal mobile phones and smart watches

There are safeguarding risks to children associated with the use of personal mobile phones and smart watches. **Once upon a time** 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.

- ★ Personal mobile phones are to be stored securely in the pockets supplied in staff rooms and office areas.
- ★ Personal phones are not allowed to be used while staff are using the nursery computers in any of our office areas.
- ★ Personal mobile phones are always to be stored on silent mode or switched off.

- ★ Personal mobile phones are not to be used to conduct any work for **Once upon a time** nursery school.
- ★ Personal phones are not allowed to be connected to the settings Wi-Fi at any time.
- ★ Staff are not permitted to wear smart watches or any other device which can receive and send messages or take photographs in our nursery rooms. Other fitness devices may be worn. This is strictly at the Nursery Managers discretion.
- ★ Smart watches are not allowed to be connected to the nursery Wi-Fi at any time if worn in staff only areas.
- ★ With ongoing technology advances, the nursery reserves the rights to request the removal of any digital watch if it deemed a safeguarding risk to children.

Nursery equipment

Nursery laptops and tablets

Where staff are using a nursery laptop or tablet, they may only be used for nursery purposes.

- ★ It is the staff member's responsibility to always log onto a secure network if they are using the laptop or tablet outside of nursery.
- ★ They must not log into any personal accounts on a nursery laptop or tablet.
- ★ If a student is using their own laptop for studying purposes, they may log into the nursery Wi-Fi while they are at the nursery. They must log out of the nursery Wi-Fi if they use the laptop for personal use.
- ★ If visitors to the nursery e.g. tutors or inspectors, are using a tablet or laptop they must have the camera covered at all times.
- ★ Designated Safeguarding Leads will regularly check the browser history of nursery tablets and computers.

Nursery computers

- ★ Staff with **Once upon a time** emails must not use these for personal reasons.
- ★ Staff must not download from any internet sites unless they have the managers permission to do so.
- ★ Staff must not use **Once upon a time** computers to visit personal social media accounts of any kind.
- ★ Staff and students will be asked to sign an Online Acceptable Use Agreement

Smart TVs

The use of a television is very limited within our settings.

We do not have a TV Licence.

- ★ Staff are not permitted to login to personal accounts on our TVs.
- ★ TVs are only used to enhance learning related to themes/topics within the nursery.
- ★ Screen times are limited to a short time, appropriate to the child's age.
- ★ All 'You Tube' videos will be vetted, to check suitability, by staff **before** the children watch them.
- ★ Watching any programmes shown will always be supervised by a member of staff.
- ★ All programmes are suitably age related.
- ★ The DVD player will **only** be used on occasions as a 'down time', either after an event or after teatime.
- ★ DVDs are usually related to a story book or favourite character and do not generally last longer than 20 minutes.

Smart speakers

Smart speakers will only be used for appropriate educational opportunity, e.g. storytelling, children's songs to support group times, ethnical music, games, exercise, research facts to support learning etc.

They are not used for adult radio stations as content may not be appropriate.

Staff are not allowed to login to personal accounts.

Adults will always supervise when used, including operation of the equipment.

Platforms for online abuse and types of abuse

Online abuse can happen anywhere online that allows digital communication, such as social networks, text messages, messaging apps, email and private messaging, online chats, online gaming and live streaming sites. Children may experience several types of abuse online: Click on any of the following for more information:

★ 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.

Responding to online abuse and how to report it

The **Online Safety Lead** 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 Online Safety Lead will consider what action to take and seek advice from the Norfolk Children's Advice and 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.

Sources of support on Online Safety

UK Safer Internet Centre

For free, independent, expert advice on dealing with internet safety problems contact the Safer Internet helpline:

Telephone: 0344 381 4772
Email: helpline@saferinternet.org.uk

Childnet

For online safety information and advice for professionals working with children and young people, contact Childnet:

Telephone: 020 7639 6967
Email: info@childnet.com

Internet Matters

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

We also have information covering how we safeguard children in the following policies:

- ★ Safeguarding Policy
- ★ Technology Policy
- ★ Social Media Policy
- ★ Tapestry Policy
- ★ Nappy changing and Toileting Policy.

This Policy was adopted by Once upon a time nursery school

Date: 11 March 2024

Amended on:

Signed on behalf of the nursery

To be reviewed: As and when matters arise