

Online Safety Policy

This policy provides guidance on how our organisation uses the internet and social media, and the procedures for doing so. It also outlines how we expect the staff who work for us, and the children who are member of our community, to behave online.

As an organisation, we commit to implementing this policy and addressing any concerns quickly and within these guidelines.

Aims

The aims of our online safety policy are:

- To protect all children involved with our organisation and who make use of technology (such as mobile phones, games consoles and the internet) whilst in our care.
- To provide staff with policy and procedure information regarding online safety and inform them how to respond to incidents
- To ensure our organisation is operating in line with our values and within the law regarding how we behave online.

Understanding the online world

As part of using the internet and social media, our organisation will:

- Assess and manage the safety aspects – including what is acceptable and unacceptable behaviour for staff and children when using websites, social media including Facebook, TikTok, Instagram, Twitter or Snapchat, apps and video conferencing platforms including Zoom or Skype.
- Be aware of how staff in our organisation and the children they work with use social media both inside and outside of our setting.
- Ensure that we adhere to relevant legislation and good practice guidelines when using social media or video conferencing platforms
- Provide training for the staff responsible for managing our organisation's online presence.
- Regularly review existing safeguarding policies and procedures to ensure that online safeguarding issues are fully integrated, including:
 - Making sure concerns of abuse or disclosures that take place online are written into our reporting procedures
 - Incorporating online bullying ('cyberbullying') in our anti-bullying policy.



Managing our online presence

Our online presence through our website or social media platforms will adhere to the following guidelines

- ✓ All social media accounts will be password -protected, and at least 2 members of staff will have access to each account and password
- ✓ The account will be monitored by at least two designated member of staff in order to provide transparency, who will have been appointed by the organisation.
- ✓ The designated staff managing our online presence will seek advice from our designated safeguarding lead to advise on safeguarding requirements
- ✓ Designated staff will remove inappropriate posts explaining why, and informing anyone who may be affected.
- ✓ Our account, page and event settings will be set to 'private' so that only invited members can see their content
- ✓ Identifying details such as a child's home address, school name or telephone number should not be posted on social media platforms
- ✓ All transferring of information will be done through Switch Egress.
- ✓ Any posts or correspondence will be consistent with our aims and tone as an organisation
- ✓ Parents will be asked to give their approval for us to communicate with their children through social media, via video conferencing platforms or by any other means of communication
- ✓ Parents will need to give permission for photographs or videos of their child to be posted on social media
- ✓ Video conferencing sessions will be password protected in order to maintain children's privacy and prevent exposure to inappropriate or harmful content by third parties.

What we expect of our staff

- ✓ Staff should be aware of this policy and behave in accordance with it
- ✓ Staff should seek the advice of the designated safeguarding lead if they have any concerns about the use of the internet or social media
- ✓ Staff should communicate any messages they wish to send out to the designated person responsible for the organisation's online presence

- ✓ Staff should not communicate with children via personal accounts.
- ✓ Staff should not 'friend' or 'follow' children from personal accounts on social media and maintain the same professional boundaries online as they would in person when using organisation accounts
- ✓ Staff should make sure any content posted on public personal accounts is accurate and appropriate, as children may 'follow' them on social media
- ✓ Rather than communicating with parents through personal social media accounts staff should choose a more formal means of communication such as face-to-face, in an email or in writing, or use an organisational account or website
- ✓ Staff should avoid communicating with children via email or organisational social media outside of normal working hours
- ✓ Emails or messages should maintain the organisation's tone and be written in a professional manner, e.g. in the same way you would communicate with fellow professionals, avoiding kisses (x) or using slang or inappropriate language
- ✓ Staff should not delete messages or communications sent to or from organisation accounts children use and how to report or remove inappropriate content online
- ✓ Any concerns reported through social media should be dealt with in the same way as face-to-face disclosure, according to our reporting procedures
- ✓ At least one parent must be present during the delivery of any activities via video conferencing platforms at home.
- ✓ Any delivery of activities for children via video conferencing platforms will be supported by an additional member of staff (even if they are not actively delivering, to ensure transparency)
- ✓ Staff and children must not engage in 'sexting' or send obscene pictures to anyone.

What we expect of our children

- ✓ Children should be aware of this online safety policy and agree to its terms
- ✓ We expect children's behaviour online to be consistent with the guidelines set out in our acceptable use statement
- ✓ Children should follow the guidelines set out in our acceptable use statement on all digital devices, including smart phones, tablets and consoles.

What we expect of our parents

- ✓ Parents should be aware of this online safety policy and agree to its terms



- ✓ Parents should protect all children's privacy online and think carefully about what content they share about their child online, where they share it and who they are sharing it with.
- ✓ We expect parents 'behaviour' online to be consistent with the guidelines set out in our acceptable use statement and in our codes of conduct for parents.

Using mobile phones or other digital technology to communicate

When using mobile phones (or other devices) to communicate by voice, video or text (including texting, email and instant messages, such as WhatsApp or Facebook Messenger), we will take the following precautions to ensure children's safety{

- ✓ Staff will avoid having children's personal mobile numbers and will instead seek contact through a parent.
- ✓ We will seek parental permission on each occasion we need to contact children directly, the purpose for each contact will be clearly identified and agreed upon
- ✓ A method of accountability will be arranged, such as copies of texts, messages or email also being sent to another member of staff or to parents
- ✓ Smart phone users should respect the private lives of others and not take or distribute pictures of other people if it could invade their privacy
- ✓ Staff should have a separate phone from their personal one for any other contact with parents or children.
- ✓ Texts, emails or messages will be used for communicating information – such as reminding children or young people about upcoming events, and not to engage in conversation.
- ✓ If a child misinterprets such communication and tries to engage a staff member in conversation, the member of staff will take the following steps:
 - ✓
 - End the conversation or stop replying
 - Suggest discussing the subject further at the next teaching session
 - Inform the organisation DSL in the interest of transparency
 - If concerned about the child, provide contact details for the DSL and report any concerns using the organisations procedures

Further information for parents about keeping children safe online

LTS Group has purchased an online safety platform and encourages all parents whose child is being supported by LTS to take part in this FREE training. Please contact Liz Feeney tel: 07719 304301 for further details on how to access the training.

NSPCC The NSPCC's guidance for parents on online safety
nspcc.org.uk/keeping-children-safe/online-safety



Child Exploitation and Online Protection Centre (CEOP) Child Exploitation and Online Protection Demand's website ceop.police.uk

The UK Safer Internet Centre Safer Internet Centre's advice for parents and children saferinternet.org.uk

Contact	Contact details	Comments
Landline	020 8629 3655	Office hours
Eddi Banks	07540 881687	Director
Karen Coles	020 8629 3655	Compliance Manager
Liz Feeney	07719 304301	Safeguarding Officer
Email contacts	e.banks@ltsg.co.uk ; k.coles@ltsg.co.uk ; l.feeney@ltsg.co.uk	

SIGNED: *Eddi Banks*

POSITION: DIRECTOR

DATE SEPTEMBER 2023

REVIEW DATE: SEPTEMBER 2024