KidCare4U
Supporting children and families
Charity No. 1185496

Digital Safeguarding

Safeguarding is at the heart of everything we do in Kidcare4u.

We have a responsibility to protect and promote the safety and wellbeing of children and adults as we help them reach their full potential.

We are committed to the welfare and safeguarding of all clients, volunteers, and staff both offline, and online. And as part of this we believe it is important we can demonstrate best practice in digital safeguarding.

This policy sets out the expectations for all clients, volunteers, staff, associated contractors, third party providers and users to ensure the protection of children, young people and volunteers and staff online.

It is our responsibility to raise concerns and report online incidents that happen inappropriately, using this policy and its procedures.

Staff and anyone who uses a @kidcare4u.co.uk email address or other email address managed by Kidcare4u must follow the Acceptable use policy.

Additional safeguarding measures must be put in place to minimise specific online risk.

What this policy covers

This policy specifically covers all Kidcare4u online and digital activities, plus all digital activities undertaken on behalf of Kidcare4u.

This includes but is not limited to email; social media channels (such as Facebook, Twitter, YouTube, Instagram, WhatsApp, Tok-tok, LinkedIn); all blogging platforms; volunteer platforms; and other digital platforms such as Google Hangouts and Zoom; all ICT devices (including phones) and internet connectivity that is provided by Kidcare4u.

This policy explains our approach to protecting clients, including children, volunteers, and staff. We are constrained by the terms of service of third-party social media providers in our approach. We promote safe use, but we also recognise that some issues will only be able to be handled by the service provider and the user themselves.

Digital safeguarding principles

To uphold these principles our volunteers, clients and staff must:

- Ensure that social media accounts are set up appropriately.
- Make it clear on personal social media accounts using disclaimers that their views, thoughts and opinions are personal and not reflective of Kidcare4u policies, procedure, or guidance.
- Make sure that technical solutions are in place to reduce access to inappropriate content on devices owned or used by Kidcare4u. These could be filtering or monitoring software for example parental controls.
- Ensure the correct permissions are in place before taking and using photographs on mobile devices.

- Delete pictures after the event and in accordance with the Kidcare4u privacy policy.
- Make sure that they have parental permissions before contacting any child under 14 years of age, even if they have contacted you first.
- Make every effort to ensure that children understand why and how they must use social media responsibly and safely using the appropriate privacy settings.

We recognise that digital safeguarding is an important part of all our work, and we are committed to always delivering best practice.

We will:

- Ensure our projects, activities, and programmes support all our clients, volunteers, and staff to stay safe online.
- Use best practice digital safeguarding for technical solutions, processes, and procedures.
- Help our volunteers to support members in being effective online.
- Take best practice action when a digital safeguarding incident occurs.
- Support and train appropriate volunteers and staff in digital safeguarding.
- Have appropriate links with key organisations to raise awareness and refer and report incidents.
- Risk-assess all projects, initiatives, programmes, activities, services, and campaigns to make sure appropriate digital safeguards are in place.

Designated Safeguarding Lead

As a client, volunteer, or staff member, if you know of an allegation, concern, or disclosure incident you must inform the Designated Safeguarding Lead- Rusna Begum.
When an incident happens, we will deal with it the same way as other safeguarding incidents.
Refer to our *Safeguarding Policy*

What do we mean by digital safeguarding?

Digital safeguarding means: 'the protection from harm in the online environment through the implementation of effective technical solutions, advice and support and procedures for managing incidents'.

This means protecting our clients, volunteers, and staff from online harms such as:

- Online bullying and harassment
- Sexual exploitation and grooming online
- Discrimination and abuse on the grounds of any protected characteristic
- Sharing of illegal and inappropriate imagery
- Cyberstalking
- Impersonation and hacking
- Disinformation and misinformation
- The oversharing of personal information

The Law

Kidcare4u adheres to all relevant UK laws relating to users of our digital platforms, third party social media and the use of our ICT equipment.

Relevant laws include:

- Protection from Harassment Act 1997
- Malicious Communications Act 1988
- Communications Act 2003
- Sexual Offences (Amendment) Act 1992
- Computer Misuse Act 1990
- The Equality Act 2010
- Serious Crime Act 2015
- Data Protection Act 2018

This list is not exhaustive. We review any changes in legislation to make sure we are compliant.

Breaches in this Policy

Any breach of this policy by volunteers will be managed under the Volunteering_Policy

Any breach of this policy by staff will be managed under the staff disciplinary procedure.

Digital Safeguarding Procedures

The online space is an increasingly important area of our work and we recognise the opportunities and challenges that this brings.

Kidcare4u supports our clients in developing their digital skills, through a wide range of programmes and activities. We use third party social media channels like Twitter, Facebook, and digital platforms such as the Kidcare4u website to engage with children, funders, parents/carers, and volunteers. Staff and volunteers also use social media and the internet to communicate with one another, and with our clients and parents/carers.

We want to continue to provide a safe space for everyone to explore and communicate online, so it is important that we understand the risks and issues that the online space brings and have the appropriate procedures in place.

Mitigations – managing the risk.

A range of measures are in place to mitigate and manage online risks

- Minimising the personal information that is shared on third party social media channels.
- Seeking permission to share information about clients, children, and volunteers where appropriate.
- Supporting volunteers in setting up social media channels effectively.
- Removing and blocking offensive posts, comments, and imagery.
- Supporting and advising clients, volunteers, and staff about how to block, and remove offensive posts, comments, and imagery.
- Supporting clients, volunteers, and staff to block and report online bullying.
- Supporting clients, volunteers, and staff to remove users who break these rules.
- Encouraging the reporting of abuse.
- Supporting clients and volunteers, when, an online bullying incident occurs.
- Report allegations to police and support others to report to the police.
- Signposting users to additional support services.

- Referring victims of online abuse to additional support.

See our *Safeguarding policy and procedures*, and *Data Protection Policy* for more information.

Acceptable use of ICT, the internet, social media, mobile phones, and digital technologies

We need to make sure that all clients, volunteers, staff, and the children we work with, know what is acceptable and unacceptable when using digital technology. You must follow these procedures.

Use of Kidcare4u equipment by members and volunteers

Where there is access to Kidcare4u devices, and devices are owned by Kidcare4u, there must be necessary mitigations in place to protect clients and volunteers. These include:

- Technical solutions to reduce access to inappropriate content. These could be filtering or monitoring software, for example parental controls or up to date security software.
- Agreement to use the equipment safely, securely, and responsibly.

Users of Kidcare4u equipment should never:

- Share, download, print or distribute any content that is defamatory, obscene, indecent, pornographic, offensive, discriminatory, sexual, or violent or any other content that may cause harassment, alarm, or distress.
- Use any Kidcare4u equipment to cause harassment, alarm, or distress to others.

Where access is offered or managed by Kidcare4u to children, there is age appropriate supervision and quality assurance. Also, make sure that security and safety settings have been installed at the set-up stage. You should refer to the manufacturers best practice guides for full information.

Use of mobile phones by Kidcare4u volunteers and staff

Personal mobile phones must be used to take photographs of clients or children.

Personal mobile phones must not be accessed, unless it is an emergency call, during Saturday Kids' Club

If staff or volunteers do use their personal devices for Kidcare4u business, they must have permission from the Chief Executive Officer and they must follow the rules below and they must get permission from parents/carers before they take photos or share images.

Staff & Volunteers should always:

- Gain permission before taking pictures.
- Delete pictures from your personal device once they have been used for the purpose that they were taken for or 14 days after the event has taken place. You must check personal cloud back-ups and make sure that pictures are deleted from here as well.
- Make sure that phones and other electronic devices that

hold Kidcare4u data are password protected.

Staff or volunteers should never:

- Take photos of children using your personal mobile phones without the explicit permission of parents or carers.
- Share imagery or personal information about children or other clients on social media or the internet without consent of parent or carers.

Use of mobile phones by children

Children may bring their mobile devices to activities. During Saturday Club the use of mobile phones is not permitted, however in some activities, it may be permissible to allow the use of mobile phones by children and if so:

Children should always:

- Use their mobile phone appropriately and responsibly.
- Seek permission to share photos/imagery and videos.

Children should never:

- Use their device to bully, harass, alarm, distress or harm another child, member of staff or volunteer. or a volunteer
- Share images or videos on social media without permission.
- Access, download, view or distribute inappropriate, pornographic, discriminatory or hate material.
- Contact staff or volunteers directly without their parents/carer's permission, except in an emergency.

Use of the internet and social media by staff and volunteers

Staff and volunteers should always:

- Make it clear on personal social media accounts - using disclaimers - that their views, thoughts, and opinions are personal to them and not reflective of Kidcare4u policies, procedures, or guidance.
- Check any facts that are shared to avoid misinformation.
- Check that those responsible for the management and operations of Girlguiding social media accounts have set them up appropriately.
- Report and record online incidents appropriately.
- Act in accordance with the Kidcare4u Code of Contact
- Ensure that users are appropriately managed in accordance with the procedures set out here and all community guidelines and terms and conditions set out by third party social media providers

Staff and volunteers should never:

- Post or share information including imagery that is discriminatory, of a sexual nature, pornographic, obscene, violent, or offensive content that may cause distress, harassment or alarm to others or bring Kidcare4u into disrepute.
- Share opinions which may be viewed as discriminatory abuse against anyone on the basis of the protected characteristics defined by the Equality Act 2010. These are age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or

belief, sex, and sexual orientation.
- Share photographs or communicate with children via social media privately without parent or carer permission.
- Contact volunteers who are under the age of 14 directly using social media (via their personal accounts) without their parents or carers permission.

Use of the internet and social media by children

Children should always:
- Use social media responsibly and safely.
- Use the appropriate privacy settings.

Children should never:
- Send friend requests or follow staff and volunteers individually/personally.
- Use social media inappropriately or if they are underage.
- Bully, harass, intimidate, alarm or cause distress to another person using social media.
- Share pornographic, sexually explicit, or inappropriate material.
- Post and share photos without the permission of the parents/ carers of other children.

Use of technology for virtual meetings/activities by staff and volunteers

Virtual meetings/ activities must always be attended by 2 members of staff or volunteers, and where possible recorded. The virtual meeting organiser / Admin will monitor the meeting and behaviour.

Although most of the virtual activities we undertake are with children, the procedures below also refer to Virtual Meetings with clients, staff members or volunteers.

Staff and volunteers should always:
- Get written permission from parent/carer for children to join in.
- Use the parent/carers online account unless the child meets the age restriction for the platform you are using.
- Be dressed appropriately. Uniform is not necessary, but everyone must be fully dressed in clothing that covers top and bottom halves of the body.
- Check the environment that you are broadcasting from is suitable. Try to avoid making calls from bedrooms, but if this is not possible then blur the background or add a virtual background or position the device so that only a small part of the room can be seen.
- Ensure that members of your household are dressed appropriately - fully dressed in clothing that covers top and bottom halves of the body - or remain out of the background.
- Make sure that an appropriate adult is in the room with a child during the call if they are a under 14.
- Make sure that an appropriate adult is in the vicinity during the call if they are 14 or over.
- Make sure that a minimum of two adult volunteers are present throughout the video call - this also applies to break out rooms if they are being used.

- Staff or Volunteers must have a DBS check and have safeguarding training.
- Stay online until all children have safely left the meeting.
- Check the terms and conditions of social media sites to make sure they are suitable for the children in the group.
- Check that materials that you share with your children are suitable and age appropriate.

Staff & Volunteers should never:

- Contact children under 14 directly
- Be in a one-one conversation with a child through video messaging
- Contact a child or parent/carer using online virtual meeting calls outside of the pre-arranged meeting time

Use of technology for virtual meetings/activities by Children

Children should always:

- Have an appropriate adult with them in the same room if they are under 14 and involved in a video call.
- Have an appropriate adult in the vicinity if they are 14 or over and involved in a video call.
- Be fully dressed in clothing that covers top and bottom halves of the body.
- Try to avoid making calls from their bedrooms, but if this is not possible then blur the background or add a virtual background or position the device so that only a small part of the room can be seen.

Children should never

- Be in a one to one conversation with a member of staff or volunteer

Support organisations

These organisations offer additional support on a range of digital and safeguarding topics:

- Childline
- Samaritans
- True Vision
- Safer Internet Centre, includes The Internet Watch Foundation
- Get Safe Online
- Thinkuknow, by NCA-CEOP
- Childnet
- NSPCC Net Aware