# E- Safety Policy and Procedures (Includes Photography, Video, Mobile Phone)


**Aims**

- To be clear on the responsibilities of management and staff when using cameras, mobile phones, computers and games consoles at the Club.
- To safeguard children's welfare in relation to the above areas and minimise the risk of harm.
- To fulfil legal duties in relation to personal data and other areas, e.g.The Data Protection Act 1998

**Procedures**

**Digital and video images**

- Written permission from parents/carers will be obtained and documented before any images of children are recorded. Generally permissions are sought at the beginning of the school year accompanying the child's registration. This may mean that separate permissions are needed for:

    a. Use of images on Club website or other publicity.
    b. Images recorded during events/ parties/ fundraising or outings.

Parents must be made fully aware of how any images of their children may be used or must have the right to decide if they wish their children to be photographed. Parents must be able to have a say in how these photos will be used.

.

- Digital images will be stored in a separate file on the computer, which is accessed by Club staff only. These images must be stored in accordance with data protection laws e.g. password protected files, cameras and memory sticks locked away.

- While using digital images, staff should be aware of the risk associated with taking, using, sharing, publishing and distribution of images.

- Club staff must only use the Club equipment: personal equipment must NOT be used to record images of the children.

- Staff should be vigilant when taking digital/video images of the children to ensure that they are appropriately dressed.

- Children's names/full names will not be used anywhere on the Club's website or literature.

- After any photograph which has been on display is taken down it will be either stored in the child's file, returned to the family or shredded

**Mobile phone usage**

- The Club uses mobile phones in ensuring children are kept safe and so parents can communicate with the Club. This is particularly important when collecting the children from school and on off-site trips.
- The Club mobile phones will all be secured with a passcode and will be used by the Play Facilitator or Deputy only, unless a Playworker has been directed in a specific task e.g. calling an emergency contact.
- Use of the Club mobile phones will be for business and emergency purposes only and members of staff are not to be distracted from the care of children. The phones can be checked at any time by the Play Faciliator to ensure this rule is being followed.
- All staff will keep their phones switched off at all times when working with children at the Club, or they may keep them in the office out of sight and reach of children.
- Staff may only use their mobile phones at Holiday Club during their designated breaks and in an area away from the children.
- The Club's contact number will be given as an emergency number if staff members need to be contacted.
- Club staff must never exchange mobile phone numbers with children in the Club.
- Club staff are not to use personal mobile phones or cameras to photograph the children.
- Images taken of the Club or its children should be downloaded onto the Club computers only. Images must not be downloaded onto any personal computer.
- Visitors and parents will be asked not to use phones while on the premises this request will be made in our registration information packs and also via posters at the Club.
- Offsite on outings, mobile phones may be very useful. Where child information is stored on a personal mobile for an outing this needs to be deleted after the outing is over. It is recommended for the senior member of staff to record this occurrence. Alternatively paper information may be taken on outings.

**Computer, laptops and tablets**

- Staff should not use the Club's computers for personal use.
- The Club will ensure that all programs used and websites accessed are appropriate and that children are not able to access or download material which is unsuitable.
- Passwords used on laptops accessed by the children should be unrelated to those used by the Club for business purposes.
- All Club files that contain personal data will be stored appropriately and securely, e.g. password protected or locked away.

- All ICT equipment should remain in the Club at all times. This is to minimise the risk of computer viruses and for data protection purposes.
- Staff should not access, copy, remove or otherwise alter any other user's files, without their expressed permission.
- All email communication should be appropriate and written in a professional manner.
- Caution should be taken if personal e-mail addresses are used on the Club computer.
- E-mail attachments should only be opened if they are from a source known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- Illegal or inappropriate materials MUST NOT be uploaded, downloaded or accessed.
- Staff should ensure that Club's computers are used appropriately to avoid disabling or damaging equipment.

**Working from home**

Staff may work from home and they can use their own device or communications equipment. Data protection law doesn't prevent thatbut there are some security measures for homeworking to take into consideration:

- Staff should not forward any of the Club work, files, information etc stored on the Club computer to their home PC, unless, this has been agreed by management as necessary practice for the Club. Any work taken home needs to be appropriately protected as if it were in the Club and open to scrutiny by management.
- Staff should not use any personal memory devices in the Club's computers. Memory sticks provided by the Club should be used for work purposes only and if taken off the premises must be encrypted and password protected

**Social networking sites**

- Staff, volunteers, students, registered bodies etc should not put details of their work on any form of social networking site.
- Staff, volunteers, students, registered bodies etc. should not engage in any on-line activity that may compromise their professional responsibilities.
- Photographs, names of, or comments about children within the Club must never be placed on any social networking site, except those controlled by the Club with appropriate privacy settings.
- Adults working with children/young people should not correspond with the Club's children/families through social networking sites.
- Members of staff should be aware of possible implications when entering any personal details on any gaming or social networking sites (e.g. YouTube, Facebook, twitter etc). If we should enter any information we MUST have prior permission from parents to do so.
- The Club's computers should only be used for Club related activities. Staff will not be permitted to use the equipment to access social networking sites at any time, including designated breaks.

- All communications in the Club should be transparent and open to scrutiny.
- All staff should be made aware that failure to comply with policies and procedures may result in disciplinary action being taken.

**Mobile phones usage for children**

We ask that children do not bring mobile phones or handheld devices. If this is unavoidable we recommend that the child gives the phone or console to the staff for safety. If a phone or console is not handed in it must be kept in the bag, turned off. If this is not the case it will be removed and handed back at the end of the session.

**Games consoles**

- Staff should ensure that all games consoles and games used are suitable and appropriate for the ages of children in their care.
- Use of computer consoles should be supervised and monitored and children encouraged to participate in a broad range of activities.
- All games used should be originals and not copies.
- Parents/carers should be made aware that computer games are available and have the option to request that their child does not access this equipment.

Children should be closely supervised to ensure that they are not accessing the Internet via the console. Or if they are permitted to do so that the websites accessed are appropriate and the Club has put in place appropriate safeguards.

**Responsibilities**

This means that adults/playworkers/employees should:

- Report any concerns about any inappropriate or intrusive photographs found or any activity that raises concerns.
- All staff should be made aware that failure to comply with policies and procedures may result in disciplinary action being taken.
- Be aware that not following Club guidance is potentially a child protection issue which may affect their suitability to work with children.

**Further Information**

South West Child Protection Procedures – provide detailed online information on all aspects of child protection – www.swcpp.org.uk

Guidance for Safer Working Practice for Adults who work with Children and Young People - DCSF (PDF held at Club)

Data Protection www.ico.gov.uk

**DOCUMENT HISTORY**

| Reference | Author | Summary of changes | Issued |
|---|---|---|---|
| Issue 1 | Raquel de Mena/Emma Hallett/Ann Charlotte | Original Version based on policy from BAND | Sept 2012 |
| Issue 2 | Sheila Gould | Reviewed to reflect Muller Road and Brunel Field ASC sites | November 2013 |
| Issue 3 | Sheila Gould Raquel De Mena | Social Media Policy reviewed and amended. Links reviewed and updated. Minor changes. | December 2014 |
| Issue 4 | Raquel de Mena | No change | November 2016 |
| Issue 5 | Aimee Bowden | No change | October 2019 |
| Issue 6 | Rakel de Mena | Added 'working from home section' | Feb 2021 |

**Date Approved:** 1/6/21

**Signed:**

**Position: Trustee** **Name: J.Hodgson**

**Date for review: Feb 2022**