NETHER GREEN JUNIOR
AFTER SCHOOL CLUB
Safeguarding children

e-Safety Policy

Policy Statement

At Nether Green Junior After School Club we take our role of safeguarding seriously. We use online processes to accept new starters, as well as sending out invoices and do most of our recruitment online. We also have a mobile phone, so that the parents/personnel can contact the manager out of opening hours and it is also used to check emails when on site. There is a laptop computer for the club and is kept at the manager's home. This is password protected and nobody else has access to it. There is also a spare (purple laptop) kept onsite for deputies to use for admin jobs. The deputies log on user only has access to sensitive information regarding the children's health and dietary needs. Deputies do not have access to the club email or any other files than previously mentioned. This is password protected and locked away when not in use. *A company device is defined as a device not used for any personal reasons.*

This policy applies to all members of this Setting (including committee, managers, staff, students on work placement, volunteers, children and young people, mothers and fathers / carers, visitors, community users) who have access to and are users of communications technologies (whether these belong to this Setting or to the users themselves). Safeguarding is considered everybody's business and online safety is not the sole responsibility of one individual. An agreed, shared approach must be promoted by all.

The following four sections outline the roles and responsibilities for the online safety of users within the setting.

- NGJASC policies and guidance are available to all. Staff, volunteers, students and all users should be aware of these guidelines.

- Staff, volunteers, students and users are also governed by relevant legislation, which is referred to in this policy and by the guidance provided by the Sheffield Children Safeguarding Partnership (with regard to safeguarding/child protection and how incidents should be reported).

Management Committee:

- The Management Committee Chair has overall responsibility for ensuring the safety (including online safety) of all children and young people, staff, volunteers, students and members of the setting. This can be done by delegating a person of responsibility to be the Online-safety coordinator.

- The Management Committee Chair, the Manager and deputy should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff or volunteer.

- The Management Committee is responsible for ensuring that the online-safety coordinator and other relevant staff / volunteers/ students have access to suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
    - The online-safety coordinator should undertake online safety training.

- The Management Committee will ensure that there is a system in place to allow for the monitoring of online safety in the setting and that they receive regular monitoring reports.

NETHER GREEN JUNIOR
AFTER SCHOOL CLUB

.

Online-safety Coordinator: Tammy Nelson

ensures that all staff / volunteers / students are informed of e-safeguarding policies and procedures as part of the induction process and that access to information and systems are withdrawn on leaving the setting's employment.

- ensures that staff / volunteers / students have an up-to-date awareness of the club's current e-safeguarding policy and practices.
- ensures that children and young people are supported to learn about online safety in a way which is appropriate for their age and development.
- ensures that all staff / volunteers / students are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies / documents
- keeps up to date with developments in online safety & offers advice and support for all users, including communicating with mothers and fathers / carers
- understands and knows where to obtain additional support and where to report issues
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments. Monitors incident log & reports regularly to the Management Committee
- ensures provision of training and advice for staff, volunteers and students

Staff, Volunteers and Students

are responsible for ensuring that:

- they have an up-to-date awareness of the setting's current online safety policy, guidelines and practices
- they report any suspected misuse or problem to the manager or deputy particularly where it is believed that a child's welfare is at risk.
- Children and young people in their care are aware of online safety issues particularly those related to the use of mobile phones, cameras, gaming consoles and hand-held devices and that they monitor their use and implement the club's policies with regard to these devices.

Children and young people do not have access to the internet at the club and are to hand in their mobile phones, hand held devices etc on arrival which we keep safe until they are collected.

Mothers and Fathers / Carers

Mothers and fathers / carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in a safe and appropriate way. Research shows that many mothers and fathers / carers do not fully understand the issues and can be less experienced in the use of communications technologies than their children.
The setting should therefore take every opportunity to help them understand these issues.

- Mothers and fathers / carers should sign the relevant permission forms on the taking and use of digital and video images.
- Mothers and fathers /carers should be aware of and adhere to the club's policies in relation to the use of mobile phones/personal devices and the taking of photographs/video images.
- It is the school's policy for the whole of the school grounds to be a mobile free zone. NGJASC enforces this policy in regards to personal mobile phones.

NETHER GREEN JUNIOR
AFTER SCHOOL CLUB

Communication between adults and children / young people, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

When using digital communications, staff, volunteers and students must:

- only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the setting and only via the setting's equipment/devices. Use of social media to contact children is not permitted. Any attempts of contact from children to staff should be reported to the e-safety coordinator so they can speak to the child about why this is inappropriate and make sure they aren't feeling rejected.
- not request any personal information, or respond to requests to provide any personal information, from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- ensure that all communications are transparent and open to scrutiny.
- be careful in their communications with children/young people so as to avoid any possible misinterpretation.
- Ensure that any personal social networking profiles are not accessible by our children. Details of social network accounts are not shared with children and young people in our care.
- Not post information online that could harm the settings reputation or cause friction between NGJASC and it's customers.
- be aware of the sanctions that may be applied if breaches of policy relate to professional misconduct.

Any communications outside the agreed policies and procedures (above) may lead to disciplinary and /or criminal investigations.

Wider personal use of digital communications:

Everyone should be able to enjoy the benefits of digital technologies. Staff, volunteers and students should, wherever possible, seek to separate their professional online presence from their online social life and take the following into account when using these digital communications:

- Careful consideration should be given as to who should be included as "friends" on social networking profiles and which information / photos are available to those friends
- Privacy settings should be frequently reviewed.
- Creating different 'groups of friends' should be considered to control what and how much information friends can see.
- The amount of personal information visible to those on "friends" lists should be carefully managed and users should be aware that "friends" may still reveal or share this information.
- "Digital footprint" – information, including images, posted on the web may remain there forever. Many people subsequently regret posting information that has become embarrassing or harmful to them

NETHER GREEN JUNIOR
AFTER SCHOOL CLUB

ICT Systems and Access

NGJASC only allows the manager (e-safety officer) and deputy (if needed) to manage the ICT systems and have access to the databases. We do not allow children or staff to use individual computers, laptops, network systems and devices unless they have specifically requested to do so for their studies. If they do, their devices will be as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Computers and devices will be managed in ways that ensure that the setting meets accepted online safety requirements, as below:

- The use of computers and devices are not permitted onsite for children. Deputies may use the club tablet/ purple laptop and internet if needed for the running of a session. The manager always has access to the internet.
- Personal data must not be sent over the internet or taken away from the setting's offices / facilities unless safely encrypted or otherwise secured e.g. use of secure emails.
- Changes to computers/systems and devices can only be made by those who have permission to do so e.g. not installing software or changing the security on the computers.
- All equipment and devices are protected against online security threats by up-to-date anti-virus software.
- Passwords will be provided, where required, for those who need access to these computer systems / devices and access will be restricted for those who do not.
- Approval to use memory sticks / CDs / DVDs / games must be obtained before being used on the setting's computers/systems and devices.
- All staff will use walkie talkies as instructed and remain on the designated channel. No children should use the walkie talkies and sensitive information will not be shared through them.

Personal Devices

Staff (excluding the manager) are not to have their mobile phones on them unless they have been given permission to do so by the manager. Staff are asked to give out the landline number for urgent cases e.g. parental responsibilities. Phones are to be kept in the storage room.

Use of digital images and video

Photographs or video images should only be taken using club technology which is passworded. There is a digital camera available at the club. Pictures should only be downloaded from it using a company computer.

Staff, volunteers and students, children and young people and mothers and fathers / carers need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The after-school club will raise awareness about these risks and will implement policies to reduce the likelihood of the potential for harm

- Written permission from mothers and fathers / carers will be obtained to allow images to be taken of their children / young people and also allowing their use for legitimate activities or for publicity that reasonably celebrates success and promotes the work of the setting. We also ask for the children's permission to use the photo. Images with children in the background, cannot be used if permission has not been given for

those children too.

- If photographs are taken, their storage and use must not cause risk or embarrassment and should comply with current data protection laws. They should be deleted from the devices after they have been transferred to the club's computer or computer system. They will be destroyed once they are not needed.

- The full names of children / young people will not be used in the newsletters and the website, particularly in association with photographs. Consideration should be given to media coverage and where applicable, journalists should be made aware of this policy. Extra permission will be gained from both parent and child, if photos are to be used on the company website and stored within a website file.

- Staff volunteers and students are allowed to take digital / video images, where appropriate/given parental permission, but must follow this policy concerning the sharing, distribution and publication of those images. Those images should ONLY be taken on the club's equipment NOT the personal equipment of staff, students and volunteers.

- Care should be taken when taking digital / video images that children / young people are appropriately dressed and are not participating in activities that might bring the individuals or the club into disrepute.

- Photographs published on the website, or elsewhere that include children / young people will be selected carefully and will comply with good practice guidance on the use of such images*. Photos of children leaving our care will be removed e.g. leaving junior school.*

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018/GDPR which states that personal data must be:

- **Processed fairly and lawfully**
- **Processed for limited and lawful purposes**
- **Adequate, relevant and not excessive**
- **Accurate and up to date**
- **Held no longer than for the purpose it was originally collected**
- **Processed in accordance with the data subject's rights.**
- **Secure**
- **Only transferred to others with adequate protection and permission**

Data Protection Officer (DPO)

The DPO (Tammy Nelson) must be familiar with all information that is held, information risks and the organisation's response to those risks. Their role is to understand:-

- What information is held, and for what purposes
- How information will be amended or added to over time
- Who has access to the data and why
- How information is retained and disposed of
- As a result they will be able to manage and address risks to the information and make sure that information handling complies with legal requirements.

NETHER GREEN JUNIOR
AFTER SCHOOL CLUB

It is the responsibility of all staff, volunteers and students to take care when handling, using or transferring personal data so that it cannot be accessed by anyone who does not have permission to access that data or does not need to have access to that data. Anyone who has access to personal data must know, understand and adhere to this policy.

The Data Protection Act (2018) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles".

Staff, volunteers and students must ensure that:

- The filing cabinet is locked at the end of each session and report anyone trying to access the club's area in the back room at the school.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use of personal data should only be on secure, password protected NGJASC computers and other devices e.g. laptops.
- When personal data is stored on any portable computer system, USB (memory)stick or any other removable device:
    - the data should be encrypted and password protected
    - the device, should be password protected.
    - the device should have up to date anti-virus and malware checking software
    - the data should be securely deleted from the device, once it has been transferred or its use is complete.

Responsibilities

The Owner/Management Committee/Directors will keep up to date with current legislation and guidance and will carry out risk assessments where necessary.

Training & awareness

Staff, volunteers and students will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff, volunteers and students
- Meetings / briefings / training for staff / volunteers / students
- Day to day support and guidance from the Manager / Deputy.

Risk Assessments

Information risk assessments will be carried out by the Data Protection Officer and staff to establish key areas of the setting where data might be at risk and how the risk could be reduced.

Storing personal data

- Personal data must be held securely on the setting's premises and only accessed by those with permission to do so. Any personal data removed from the premises should have the appropriate level of protection to prevent loss of data as stated previously.
- The setting has clear policy and procedures for the automatic backing up, accessing and restoring all data held on systems, including off-site backups.

NETHER GREEN JUNIOR
AFTER SCHOOL CLUB

- The setting recognises that under the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access.

- Events such as, Outings, Christmas and Fundraising Events may be recorded by video and photographs by staff and parent/carers but always in full view of all attending and permission must be given by all parents and carers.

- Unmanned aerial vehicles (UAVs) or drones are the new generation of remote-controlled aircraft. Currently, the Civil Aviation Authority (CAA) sets the rules on drones in the UK under an air navigation order, which focuses on safety. An unmanned aircraft must never be flown beyond the normal unaided 'line of sight' of the person operating it: - No further than 500m (0.3 miles) from the pilot - No higher than 122m (400ft). An unmanned aircraft fitted with a camera must not be flown within 150m of a congested area or within 50m of people, vehicles or buildings. These laws mean that drones should not enter school air space and any concerns should be reported to the police on 101.

Free independent expert advice contact line:

Safer Internet Centre, tel. 0844 3814772

Email: helpline@saferinternet.org.uk

Website: www.saferinternet.org.uk

This policy was adopted at a meeting of	Nethergreen Junior After School Club
Held on	Sept 2022
Date to be reviewed	Oct 2023
Signed on behalf of the Co-ordinator	
Name of signatory	Tammy Nelson