For the benefit of this policy Laira Green Trust – which is the governing body of Greenshoots Pre-school and Wraparound care is hereafter referred to as Greenshoots.

Online Safety

As a provider we have used the Online Safety Toolkit to create policies and procedures to cover all forms of information and communication technology (ICT). This enables adults and children within the setting to communicate and learn to use ICT safely.

The policies recognise the safety and potential risks as well as the immense value of ICT. The Senior Designated Person for Safeguarding (SDPS) is responsible for ensuring the policies are put into practice.3

Policies that are in place include:

- Acceptable Use Policy
- Internet Policy
- Camera and Image Policy
- Mobile Phone Policy
- ICT Misuse Policy

We do not have CCTV so we do not have a policy dictating its use within the setting.

Further information can be found in Online Safety: A Toolkit for Early Years Settings which can be accessed through the Plymouth City Council website or via the online safety service of the South West Grid for Learning Trust.

Online compass is a simple tool that we can use to show us what we need to do to make the use of technology safer for our setting.

We take the steps necessary to encrypt electronic private data to help prevent unauthorised disclosure.

For the benefit of this policy Laira Green Trust – which is the governing body of Greenshoots Pre-school and Wraparound care is hereafter referred to as Greenshoots.

Acceptable Use Policy

Aim

The Acceptable Use Policy (AUP) will aim to:

- Safeguard children and young people by promoting appropriate and acceptable use of information and communication technology (ICT).
- Outline the roles and responsibilities of all individuals who are to have access to and/or be users of, work-related ICT systems.
- Ensure all ICT users have an acute awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.

Scope

The AUP will apply to all individuals who are to have access to and/or be users of work-related ICT systems. This will include children and young people, parents and carers, early years practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not to be considered exhaustive.

Parents and carers, and where applicable, other agencies, will be informed of any incidents of inappropriate use of ICT that takes place on-site, and, where known, off-site.

ICT available in the setting

2x tablets for educational games for children

2x tablets for staff use only for on line learning journeys

1x camera for photos to be taken by staff only

3x Children's camera

2x Apple mac laptop for adults stored in the office away from the children

2x PC's in the main room for the children

1x interactive touch screen TV

Roles and responsibilities

Registered person

The registered person is to have overall responsibility for ensuring online safety will be considered an integral part of everyday safeguarding practice.

This will include ensuring:

- Early years practitioners and their managers will receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.
- Clear and rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who affect or come into contact with the early years setting. Such policies and procedures are to include the personal use of work-related resources.
- The AUP is to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity.
- Monitoring procedures are to be open and transparent.
- Allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- Effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection.

Senior Designated Person for Safeguarding (SDPS)

The Senior Designated Person for Safeguarding (SDPS) must be a senior member of the management team who is to have relevant, current and practical knowledge and understanding of safeguarding, child protection and online safety. Access to an individual holding this role is to be available at all times, for example, a designated deputy.

The Senior Designated Person for Safeguarding will be responsible for ensuring:

- Agreed policies and procedures are to be implemented in practice.
- All updates, issues and concerns are to be communicated to all ICT users.
- The importance of online safety in relation to safeguarding is to be understood by all ICT users.
- The training, learning and development requirements of early years practitioners and their managers are to be monitored and additional training needs identified and provided for.
- An appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities where deemed appropriate.
- Any concerns and incidents are to be reported in a timely manner in line with agreed procedures.
- The learning and development plans of children and young people will address online safety.
- A safe ICT learning environment is to be promoted and maintained.

Early year's practitioners and their managers

Early years practitioners and their managers will ensure:

- The timely reporting of concerns in relation to alleged misuse or known incidents, subject to agreed procedures.

- ICT equipment is to be checked before use and all relevant security systems judged to be operational.
- Awareness will be raised of any new or potential issues, and any risks which could be encountered as a result.
- Children and young people are to be supported and protected in their use of online technologies – enabling them to use ICT in a safe and responsible manner.
- Online safety information is to be presented to children and young people as appropriate for their age and stage of development.
- Children and young people will know how to recognise and report a concern.
- All relevant policies and procedures are to be adhered to at all times and training undertaken as is to be required.

Children and young people

Children and young people will be encouraged to:

- Be active, independent and responsible learners, who will contribute as appropriate to policy and review.
- Abide by the Acceptable Use Agreement as to be approved by peers, early years practitioners and their managers, parents and carers.
- Tell a familiar adult about any access of inappropriate content, material that makes them feel uncomfortable or contact made with someone they do not know, straight away, without fear of reprimand (age and activity dependent).

Parents and carers

Parents and carers are to be encouraged to sign Acceptable Use Agreements alongside their children and to share responsibility for their actions and behaviours. This will ensure a consistent message is to be communicated to all.

A copy of an Acceptable Use Agreement is to be provided to parents and carers on enrolment of their child at the early years setting. This will be reviewed on an annual basis thereafter. It will be an expectation that parents and carers will explain and discuss the Acceptable Use Agreement with their child to ensure that it is to be clearly understood and agreed. Children and young people will also be encouraged to sign the Acceptable Use Agreement alongside their parent or carer. Records of all signed agreements are to be kept on file.

Parents and carers will also be required to sign additional Acceptable Use Agreements if they are to undertake any voluntary work within the early years setting and/or participate on associated trips or visits. Further agreement is to be sought if parents and carers are to be given remote access to ICT systems, such as a learning environment, electronic portfolio or remote webcam.

Acceptable use by early years practitioners and their managers

Early years practitioners and their managers should be enabled to use work-based online technologies:

- To access age appropriate resources for children and young people;
- for research and information purposes;
- for study support.

All early years practitioners and their managers will be subject to authorised use as agreed by the Senior Designated Person for Safeguarding (SDPS).

Authorised users will have their own individual password to access a filtered internet service provider. Users are not generally permitted to disclose their password to others, unless required to do so by law or where requested to do so by the Senior Designated Person for Safeguarding. All computers and related equipment are to be locked when unattended to prevent unauthorised access.

All early years practitioners and their managers are to be provided with a copy of the Acceptable Use Policy and a copy of the Acceptable Use Agreement, which they must sign, date and return. A signed copy is to be kept on file.

The use of personal technologies will be subject to the authorisation of the Senior Designated Person for Safeguarding, and such use will be open to scrutiny, monitoring and review.

In the event of misuse by early years practitioners or their managers

Should it be alleged, that an early years practitioner or manager is to have misused any ICT resource in an abusive, inappropriate or illegal manner, a report is to be made to the Senior Designated Person for Safeguarding and the registered person immediately. Should the allegation be made against the Senior Designated Person for Safeguarding, a report is to be made to a senior manager and the registered person.

Procedures are to be followed as appropriate, in line with the ICT Misuse Procedure, Safeguarding Policy and/or Disciplinary Procedures. Should allegations relate to abuse or unlawful activity, Children's Social Care, the Local Authority Designated Officer, Ofsted and/or the Police will be notified as applicable.

Acceptable use by children and young people

Acceptable Use Agreements are to be used to inform children and young people of the appropriate behaviours expected to ensure online safety. Children and young people will also be informed of the behaviours which will be deemed unacceptable. This will allow children and young people to take some degree of responsibility for their own actions.

In understanding Acceptable Use Agreements, children and young people will become aware of the potential risks associated with misuse and the sanctions which will be applied, where necessary.

The Acceptable Use Agreements are shared and agreed with children and young people and will be displayed as a reminder.

In the event of misuse by children and young people

Should a child or young person be found to inappropriately misuse ICT the following sanctions will be applied:

- **Step 1:** Should it be considered that a child or young person has deliberately misused ICT by not adhering to the Acceptable Use Agreement, a letter will be sent to the parent or carer outlining the issue. The child or young person may be temporarily suspended from a particular activity.
- **Step 2:** If there are to be further incidents of misuse, the child or young person will be suspended from using the internet or other relevant technology for an increased period of time. The parent or carer will be invited to discuss the incident in more detail with a senior manager and the most appropriate course of action will be agreed.
- **Step 3:** The sanctions for misuse can be escalated at any stage, should it be considered necessary. In the event that misuse is deemed to be of a serious nature, steps 1 and 2 can

be omitted. Should a child or young person be considered to be at risk of significant harm, the Safeguarding Policy must also be applied. Allegations of serious misuse will be reported to the most appropriate agency, for example, the Police or Children's Social Care.

In the event that a child or young person should accidentally access inappropriate material,it must be reported to an adult immediately. Appropriate action is to be taken to hide or minimise the window. The computer will not be switched off nor will the page be closed, as it may be necessary to refer to the site during investigations to allow effective filters to be put in place to prevent further inadvertent access.

The 'Hectors World Safety Button', is to be available to children and young people where online access is to be enabled. At a push of a button, the child's view of the screen will be obscured. Adults will immediately be alerted and should take immediate and appropriate action.

Should a child or young person be considered to be subject to potential abuse, sexual requests or other inappropriate contact, the CEOP Report Abuse button is to be used to make a report and further advice is to be sought.

Acceptable use by parents and carers

Partnership working with parents and carers should be considered essential practice for promoting an agreed and consistent message which will define acceptable and unacceptable behaviours. Parents and carers will therefore be asked to sign an Acceptable Use Agreement together with their child in order to promote this shared message.

Parents and carers are to be encouraged to contribute to the Acceptable Use Agreement and should be advised to use it should their child access similar technologies at home.

Should parents or carers wish to use personal technologies, such as cameras within the setting environment, authorisation must be obtained from the Senior Designated Person for Safeguarding. Specific guidelines for the use of such technologies must be followed.

Acceptable use by visitors, contractors and others

All individuals who affect or come into contact with the early years setting are to be expected to behave in an appropriate and respectful manner. No such individual will be permitted to have unsupervised contact with children and young people. All guidelines in respect of acceptable use of technologies must be adhered to. The right to ask any individual to leave at any time is to be reserved

Links to other policies

Behaviour Policy

The Behaviour Policy is to contain up-to-date anti-bullying guidance, which should highlight relevant issues, such as cyber bullying.

It should be recognised that all inappropriate behaviours will be taken seriously and dealt with in a similar way, whether committed on or offline. There are to be consistent expectations for appropriate behaviour in both the 'real' and 'cyber' world and this is to be reflected in all relevant policies.

Safeguarding Policy and ICT Misuse Policy

The Safeguarding Policy and the ICT Misuse Policy are to be referred to when dealing with any incidents that should occur as a result of the intentional or unintentional misuse of ICT. Any allegations of abuse or other unlawful activity are to be reported immediately to the Senior Designated Person for Safeguarding who will ensure procedures outlined in the Safeguarding Policy are followed with immediate effect.

Personal, Social and Emotional Development (PSED)

The promotion of online safety within PSED activities is to be considered essential for meeting the learning and development needs of children and young people. Key messages to keep children and young people safe are to be promoted and should be applied to both online and offline behaviours.

Health and Safety Policy

The safe use of ICT is to be included within the Health and Safety Policy, and should also include guidelines for the use of display screen equipment. The detrimental impact of prolonged ICT use on children's brain development should also be addressed.

This policy was adopted on:_____

Signed on behalf of Laira Green Trust - Greenshoots Pre-school and Wraparound Care

Chairperson, Laira Green Trust:

Greenshoots Manager (Strategy and Support):

For the benefit of this policy Laira Green Trust – which is the governing body of Greenshoots Pre-school and Wraparound care is hereafter referred to as Greenshoots.

Internet Policy

Introduction

The internet should be considered part of everyday life with children and young people seen to be at the forefront of this online generation. Knowledge and experience of information and communication technology (ICT) should be considered an essential life skill. Developmentally appropriate access to computers and the internet in the early years will significantly contribute to children and young people's enjoyment of learning and development.

Children and young people will learn most effectively where they are to be given managed access to computers and control of their own learning experiences; however such use will carry an element of risk. Early years practitioners and their managers, alongside parents and carers, should consider it to be their duty to make children and young people aware of the potential risks associated with online technologies. This will empower them with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.

Aim

The Internet Policy will aim to outline safe and effective practice in the use of the internet. It will provide advice on acceptable use and effective control measures to enable children, young people and adults to use ICT resources in a safer online environment.

Scope

The Internet Policy will apply to all individuals who are to have access to and/or be users of work related ICT systems. This will include children and young people, parents and carers, early years practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not to be considered exhaustive.

The Internet Policy will apply to internet access through any medium, for example, computers, mobile phones and gaming machines.

Responsibilities

The Senior Designated Person for Safeguarding (SDPS) is to be responsible for online safety, and will manage the implementation of the Internet Policy.

The Senior Designated Person for Safeguarding will ensure:

- Day to day responsibility for online safety issues and as such will have a leading role in implementing, monitoring and reviewing the Internet Policy.

- All ICT users are to be made aware of the procedures that must be followed should a potentially unsafe or inappropriate online incident take place.
- Receipt, recording, monitoring and filing of reports should a potentially unsafe or inappropriate online incident occur. This must include the creation of an incident log to be used to inform future online safety practice.
- All necessary actions will be taken to minimise the risk of any identified unsafe or inappropriate online incidents reoccurring.
- Regular meetings are to take place with the registered person and senior managers to discuss current issues, review incident reports and filtering/change control logs.
- Effective training and online safety advice is to be delivered and available to all early years practitioners and their managers. This should include advisory support to children, young people, parents and carers as necessary.
- Timely liaison, where appropriate, with other agencies in respect of current online safety practices and the reporting and management of significant incidents.

Further details on the responsibilities of the Senior Designated Person for Safeguarding, registered person, early years practitioners and their managers, parents and carers, children and young people are to be found in the Acceptable Use Policy.

Managing online access

Password security

Maintaining password security is to be an essential requirement for early years practitioners and their managers particularly where they are to have access to sensitive information. A list of authorised ICT users is to be maintained, and access to sensitive and personal data is to be restricted.

Early years practitioners and their managers will be responsible for keeping their passwords secure and must ensure they are to be regularly up-dated – at least once every 60 days. All ICT users must have strong passwords, for example, an impersonal combination of numbers, symbols and lower/upper case letters.

Sharing passwords is not to be considered secure practice. Where children and young people are to be enabled to create their own password however, a copy of such will be kept on file for reference.

It is to be considered good practice for computers and laptops to be set to ‘timeout’ the current user session should they become idle for an identified period. All ICT users must ‘log out’ of their accounts should they need to leave a computer unattended.

If ICT users should become aware that password security has been compromised or has been shared, either intentionally or unintentionally, the concern must be reported to the Senior Designated Person for Safeguarding.

Internet access

It is to be considered essential practice that internet access for all ICT users will be managed and moderated in order to protect them from deliberate or unintentional misuse. Every reasonable precaution will be taken to ensure the safe use of the internet. It has to be acknowledged however, that it will be impossible to safeguard against every eventuality.

The following control measures will be put in place which will manage internet access and minimise risk:

- Secure broadband or wireless access.
- A secure, filtered, managed internet service provider and/ or learning platform.
- Secure email accounts.
- Regularly monitored and updated virus protection.
- A secure password system.
- An agreed list of assigned authorised users with controlled access.
- Clear Acceptable Use Policies and Agreements.
- Effective audit, monitoring and review procedures.

Online activity is to be monitored to ensure access will be given to appropriate materials only.

Computers and gaming machines are to be sited in areas of high visibility which will enable children, young people and adults to be closely supervised and their online use to be appropriately monitored.

Should children, young people or adults discover any potentially unsafe or inappropriate material, they are to hide the content from view. For example, the window will be minimised and/or the monitor (not computer) will be turned off. The use of the CEOP Hectors World browser button and Report Abuse button are to be considered best practice1. All such incidents must be reported to the Senior Designated Person for Safeguarding; who must ensure a report of the incident is to be made and will take any further actions which are to be deemed necessary.

All early years practitioners and their managers are to be made aware of the risks of compromising security, for example from connecting personal mobile devices to work-related ICT systems. Such use is to be avoided as far as is practically possible. Should, on occasion it be unavoidable, it will be subject to explicit authorisation by the Senior Designated Person for Safeguarding. Such use will be stringently monitored.

Should it be necessary to download unknown files or programmes to any work-related system, it will only be actioned by authorised ICT users with express permission from the Senior Designated Person for Safeguarding. All such use will be effectively managed and monitored.

All users are to be responsible for reporting any concerns encountered using online technologies to the Senior Designated Person for Safeguarding.

Online communications

All official online communications must occur through secure filtered email accounts. Web-based commercial email services are not to be considered secure.

All email correspondence will be subject to scrutiny and monitoring.

All ICT users will be expected to write online communications in a polite, respectful and non-abusive manner. The appropriate use of emoticons is to be encouraged.

A filtered internet server is to be used to monitor and prevent offensive material or spam. Should, on rare occasions, security systems not be able to identify and remove such materials, the incident will be reported to the Senior Designated Person for Safeguarding immediately.

In line with, ‘Guidance for Safer Working Practice for Adults who Work with Children and Young People’ it will not be considered appropriate for early year’s practitioners or their managers to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites under Principle Eight of the GTC Code of Practice.

Staff will not have access to social media networking sites. Sites such as Facebook are blocked so that they cannot be accessed.
Children do not have access to social media sites or emails at Greenshoots.

Communications between children and adults by whatever method should take place within clear and explicit professional boundaries. Early years practitioners and their managers should not share any personal information with any child or young person associated with the early years setting. They should not request or respond to any personal information from the child or young person other than that might be considered appropriate as part of their professional role. Early years practitioners and their managers should ensure that all communications are to be transparent and open to scrutiny.

All ICT users are to be advised not to open emails where they do not know the sender or where the format looks suspicious.

Online communication is not to be considered private or confidential for safeguarding and security purposes. Such communication is to be monitored and must be available for scrutiny at any time.

Children and young people will be enabled to use online equipment and resources, when it is to be considered, in consultation with parents and carers, that they have the developmental knowledge and understanding to recognise some of the benefits and risks of such communication. Access to online communications will always be monitored by a supervising adult.

Where children and young people are to access online communications and communities, it will be considered best practice for them to adopt a nickname which will protect their identity and ensure anonymity.

Managing multimedia technologies (including Web2 and 3G technologies)

Multimedia technologies, where they are to be used responsibly, will provide easy to use, creative, collaborative and free facilities. However, it is to be recognised that there are issues regarding the appropriateness of some content, contact, culture and commercialism.

Emerging technologies should be valued for the learning and development opportunities they will provide for children and young people; including a move towards personalised learning and one to one device ownership. Many existing technologies such as portable media players, gaming devices, and mobile phones will already be familiar to many children and young people.

Many of these devices will be equipped with internet access, GPS, cameras, video and audio recording functions. They should therefore be considered subject to the same risks as any other form of technology. Effective control measures should therefore be put in place to minimise such risk whilst maximising the opportunities for children and young people to access such resources.

Access to a range of age-appropriate websites should be enabled, but children and young people should be encouraged to be cautious about any information given to them by other users on such sites, and must recognise that not everyone is who they say they are.

Access to social networking sites is to be restricted within the early years setting, and children and young people will only be permitted to use moderated child-focused sites under supervision. Early years practitioners and their managers are not permitted to use work-related technologies for personal access to social networking sites.

All ICT users are to be encouraged to think carefully about the way information can be added and removed from websites by themselves and others. Moderated sites, through SWGfL, such as

‘Learning Platform Merlin’ and ‘My First Place’ are therefore to be used to afford maximum protection.

Children and young people will be taught to think carefully before placing images of themselves on such sites and to be aware of details within images, such as a school badge, which could reveal personal and background information. Children and young people should consider the appropriateness of any images owing to the permanency of online material.

Children and young people must always be reminded not to give out or post personal details on websites, particularly information which could identify them or provide information that would contribute to their personal profile. For example, full name, address, mobile/home telephone numbers, school details, IM/email address and specific hobbies/interests.

Children and young people are to be advised on how to set and maintain web profiles to appropriate privacy levels and to deny access to unknown individuals.

Children and young people, parents and carers are to be informed that the use of social networking sites in the home or social environment is to be seen as an exciting communication and networking tool. It must also be emphasised however that their use can pose potential risks. Children and young people, parents and carers should therefore be made aware of the potential risks, and the control measures that can be implemented to minimise them.

It is to be recognised that early years practitioners and their managers are also likely to use social networking sites in their recreational time on their own personal computers. This form of activity is not to be discouraged however early years practitioners must agree and adhere to a ‘professional conduct agreement’. It must be ensured that the use of such sites will not compromise professional integrity or bring the early years setting into disrepute. The adding of children and young people, parents and carers as ‘friends’ to a social networking site should be avoided.

It must be recognised that social networking sites and mobile technologies can be used for negative and anti-social purposes. Cyberbulling, for example, is to be considered as unacceptable as any other form of bullying and effective sanctions must be in place to deal with such concerns. Any known or suspected incidents must be reported immediately to the Senior Designated Person for Safeguarding.

Emerging technologies

Emerging technologies are to be examined to determine potential learning and development opportunities. Their use is to be risk assessed before consideration will be given to enabling use by children and young people. Where necessary, further training and guidance is to be sought to ensure appropriate and safe use of any new technologies.

Smart watches

Smart watches are the newest technology that we need to be aware of. They are considered by many as tiny smart phones on your wrist. They can be used to send and receive messages, emails, make phone calls and connect to social network sites. The latest

Some versions of the smart watches also have the ability to take photographs as there are mini cameras built into the device.

Like other computers, a smart watch may collect information from internal or external sensors. It may control, or retrieve data from, other instruments or computers.

The use of Smart watches in our provision are treated the same as mobile phones. Smart watches are not permitted at any time when working with the children. Smart watches will be stored in the office away from the children the same as a mobile phone.

It is acceptable that adults can use their smart watches on their break times away from the children the same as a mobile phone. If a member of staff is seen wearing a smart watch they will be asked to remove it immediately and store it away in the office or in the settings safe. Managers/seniors will familiarise themselves with what smart watches look like.

Smart watches must never be used to take videos or photographs of children.

This policy was adopted on:

Signed on behalf of Laira Green Trust - Greenshoots Pre-school and Wraparound Care

Chairperson, Laira Green Trust:

Greenshoots Manager (Strategy and Support)

Laira Green Trust, c/o Laira Green Primary School, Bramley Road, Laira, Plymouth, Devon, PL3 6BP. Telephone: 01752 228272.
Registered Charity No: 1136071 Registered Company No: 7110815 England & Wales.

For the benefit of this policy Laira Green Trust – which is the governing body of Greenshoots Pre-school and Wraparound care is hereafter referred to as Greenshoots.

Camera and Image Policy

Introduction

The use of cameras should be considered an essential and integral part of everyday life. As such, children and young people and early years practitioners and their managers are to be encouraged to use such technology in a positive and responsible way.

It has to be recognised however, that digital technology has increased the potential for cameras and images[1] to be misused and inevitably there will be concerns about the risks to which children and young people may be exposed.

Practical steps must be taken to ensure that the use of cameras and images will be managed sensitively and respectfully. A proactive and protective ethos is to be reflected which will aim to promote effective safeguarding practice.

It must however be acknowledged that technology itself will not present the greatest risks, but the behaviours of individuals using such equipment will.

Within the setting at Greenshoots we have:

>2x tablets for the children to use for educational games-connected to the internet
>2x tablets for adult use for Tapestry online learning journeys- connected to the internet
>1 times camera for photos of trips and outings
>3x pink children's camera
>2x computers in the main room for children – connected to the internet
>1x interactive touch screen TV – connected to the internet
>2x apple mac laptop –located in the office for managers and staff members only- connected to the internet

Aim

The Camera and Image Policy will aim to ensure safer and appropriate use of cameras and images through agreed acceptable use procedures. This is to be in line with legislative requirements and will aim to respect the rights of all individuals.

Scope

The Camera and Image Policy will apply to all individuals who are to have access to and/or be users of work-related photographic equipment. This will include children and young people, parents and carers, early years practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not to be considered exhaustive.

The Camera and Image Policy will apply to the use of any photographic equipment. This will include mobile phones and portable gaming devices with inbuilt cameras as well as other forms of digital technology and resources for storing and printing images.

Responsibilities

The Senior Designated Person for Safeguarding (SDPS) is to be responsible for ensuring the acceptable, safe use and storage of all camera technology and images. This will include the management, implementation, monitoring and review of the Camera and Image Policy. This will include all pre-school children and children who attend our breakfast and afterschool club sessions.

Further details on the responsibilities of the Senior Designated Person for Safeguarding, registered person, early year's practitioners and their managers, parents and carers, children and young people are to be found in the Acceptable Use Policy.

Legislative framework

This policy complies with the requirements of the Data Protection Act 1998, Freedom of Information Act 2000, Human Rights Act 1998 and other relevant Acts regarding the taking and use of photographic images of children.

All images will be used in a manner respectful of the eight Data Protection Principles.

This means that images will be:
• Fairly and lawfully processed
• processed for limited, specifically stated purposes only
• used in a way that is adequate, relevant and not excessive
• Accurate and up to date
• kept on file for no longer than is necessary
• processed in line with an individual's legal rights
• kept securely
• Adequately protected if transferred to other countries.

Where necessary, registration as a data controller will be applied for to allow personal information to be processed.

Images taken of children will be taken when they are involved with an activity, in full and suitable clothing, with the child's consent and in suitable areas.

Code of conduct

All early years practitioners and their managers must ensure that the policy and procedures included herein are to be adhered to at all times. The Camera and Image Policy must be considered in conjunction with the Acceptable Use Policy and the ICT Misuse Policy.

The use of cameras and other photographic equipment is only to be authorised by the Senior Designated Person for Safeguarding. Early years practitioners and their managers should only use such equipment for purposes as designated by the Senior Designated Person for Safeguarding. It must be recognised that individuals may be given different levels of responsibility in terms of authorised use.

Wherever practical, cameras and other photographic equipment will be designated for work-related purposes only. Such equipment must be booked and signed out accordingly. The use of personal photographic equipment is to be avoided. Should it be considered that such use is not to be precluded for a given reason; explicit authorisation must be obtained from the Senior Designated Person for Safeguarding and all relevant details of use are to be recorded.

Early year's practitioners and their managers must report to the Senior Designated Person for Safeguarding to book out cameras or other photographic equipment. The Senior Designated Person for Safeguarding will be responsible for ensuring that the following information is to be recorded each time equipment is booked out:

• Name of individual using the equipment.
• Date and time equipment is booked in and out.
• Type of equipment used.
• Purpose.
• Any difficulties encountered or concerns reported.

The use of personal USB sticks, the transferring of images via free unfiltered web mail or via mobile media is be avoided. Should remote access be given to servers or systems where images are to be stored, access will only be given as authorised by the Senior Designated Person for Safeguarding.

The Senior Designated Person for Safeguarding must reserve the right to view any images taken and / or to withdraw or modify an individual's authorisation to take or make images at any time.

Early years practitioners and their managers must ensure that all images are available for scrutiny and be able to justify any images in their possession.

The Senior Designated Person for Safeguarding will be responsible for ensuring the safe storage of all images, in accordance with the Camera and Image Policy.

Early years practitioners and their managers are to have a duty to report any concerns relating to potential misuse. Clear whistle-blowing procedures are to be in place. An anonymous reporting system will also be promoted and used to facilitate this process.

Consent

Statement of intent

General signed consent to take photographs or record images of children will be requested from the parent or carer on enrolment of their child. The purpose for taking any images is to be clearly explained and agreed. Any consent given is to be reviewed on a regular basis (of a period of no more than one year) until such time the child or young person will no longer attend the setting. This consent will cover the taking of images for general purposes, such as taking photographs which will be used to document children's learning.

Consent must be requested because an image of a child or young person is considered to be personal data under the Data Protection Act 1998 and consent must be obtained as a requirement of the Act. The requirement for consent will be applied to all children and young people under the age of 18 years (or from the young person, if deemed to be competent to make such a judgement, from the age of 12 years). The child's view is however to be considered at all times, regardless of age.

It should be recognised that some children and young people will be more vulnerable than others, for example disabled children, children in care, those with a child protection or child in need plan, children with English as an additional language, black, minority and ethnic children and those who have been subject to domestic abuse. For a range of reasons, such children's security may be compromised more than others, and therefore extra precautions must be considered in such circumstances.

Procedures

Prior consent will always be obtained in writing before any images will be taken. Verbal consent will not be accepted under any circumstance. If it should not be possible to obtain prior written consent, no images will be taken involving the individual child or young person concerned.

Individuals who do not have parental responsibility, such as childminders, friends or other relatives will not be able to give such consent. Only consent provided by a parent or carer with parental responsibility is to be accepted.

The parent or carer will reserve the right to refuse or withdraw their consent at any time. Partial or restricted consent may also be given where deemed necessary by the parent or carer.

Specific consent for the use of images for purposes other than those previously stated and agreed will be requested, for example, should images be required for publicity materials or to support the training needs of early years practitioners and their managers. Such consent will detail how the photographs are to be used and for what period of time such permissions will cover.

Images must not be used for anything other than the stated purposes; unless additional revised consent is to be obtained. A copy of the relevant image will be stored with the specific consent form.

Images of children who are to no longer attend the early years setting will not be used, unless specific consent has been obtained to cover this extended period. Generally consent to use images will lapse should a child leave the early years setting.

Images of children if held for which consent has never been given are not to be used, unless the specific consent of the parent or carer is to be obtained. Should it not be possible to obtain such consent, such images are to be returned to the individual concerned or destroyed.

Images

Statement of intent

It must be recognised that children and young people could be exposed to potential risk should images be misused, including:

- the making, taking and distribution of inappropriate and indecent images.
- grooming (the process by which child sex offenders and paedophiles will befriend victims through direct or indirect contact, often preceded by efforts to gain personal information about the child or young person).

It must be remembered that such incidents fortunately remain very rare; but it should also be understood that detailing such concerns will often raise further anxieties and will make many individuals feel uncomfortable. It must be acknowledged however, that the first step towards minimising any danger will be to have a fuller understanding of what constitutes a risk and what behaviours may compound it.

Protective and precautionary measures should therefore be considered when taking, making or using images of children. It is to be ensured that all early years practitioners and their managers are aware of the potential for images to be subject to misuse; and therefore will be expected to agree and sign up to an Acceptable Use Agreement (in line with the Acceptable Use Policy).

Procedures

The purpose and context for any proposed image should always be considered. It must be determined whether taking a photograph or video, for example, will be the most effective option or whether alternative methods of capturing information are to be judged more appropriate in the given circumstance.

Careful consideration must be given before involving young or vulnerable children who may be unable to question why or how activities are to take place.

Sensitivity must be shown to any child or young person who is to appear uncomfortable; and the potential for misinterpretation is to be recognised. Images will therefore not be taken of any child or young person against their wishes. Coercion must not be used to encourage a child or young person to participate when it has been indicated that they clearly do not want to be involved. A child or young person's right not to be photographed is to be respected.

The taking or making of images of a child or young person in a one to one situation with an adult is to be avoided whenever possible; unless there is an agreed, specified reason for doing so. It must be recognised that the context of such situations are likely to be perceived as sensitive and the use of cameras will be seen as intrusive and open to misinterpretation. It is to be recognised that

this may leave both the adult and child in a vulnerable position and is therefore not to be considered accepted practice.

It is to be recognised that individual close up pictures of a child or young person often provides little context or purpose, and most often, an image of a group of children will show an activity or situation to better effect. Unnecessary close up pictures of an individual child or young person with no surrounding context or purpose are therefore to be avoided. The vast majority of photographs taken in the setting environment will therefore be general shots of whole or small group activities.

Where group photographs of children and young people are to be planned, permission must be obtained from all parents and carers. If any parent or carer has indicated that their child is not to have a photograph taken then a group photograph will not be considered appropriate.

Photographs are not to be taken of any child or young person should they suffer an injury; whether it is to be considered accidental or non-accidental. This will be deemed a misuse of power which will potentially cause the child or young person to become distressed or to feel humiliated. Where necessary, medical help will be sought, and in the case of a suspected non-accidental injury the Safeguarding Policy will be implemented with immediate effect.

All images to be taken should represent the diversity of the children and young people who attend the early years setting. No child is to be favoured in photographs.

Images which could be considered to cause distress, upset or embarrassment must not be used.

Images of children and young people must only be taken when they are in full and suitable dress. In no circumstances, are images to be taken of children or young people in any state of undress. Should children and young people be participating in sport activities, careful consideration must be given to the appropriateness of taking such images, in particular the angle of which shots may be taken.

The taking or making of images in sensitive areas of the early years setting, for example, toilet cubicles and changing areas are not to be permitted.

It should be ensured that a child or young person's name or any other identifying information does not appear in any caption or accompanying text alongside their photograph, for example on displays, documentation panels etc. Particular care is to be taken where such images are likely to be viewed by others, including the general public.

It is to be ensured that if, on occasion, a child or young person is to be named (for an agreed reason) in any published text, for example, in the prospectus, a photograph of the child will not appear.

The minimum amount of information possible is to be provided to preserve the identity of children and young people at all times. No personal details, such as home telephone numbers, email or home addresses are to be disclosed in any written or verbal communications. This is to include information that will contribute to the personal profile of a child or young person.

Consideration will always to be given to where images are to be published. This will also include where parents are encouraged to be involved with learning platforms, such as 'My First Place' and 'Merlin'. These systems must be designed to enable parents and carers to access their own child's photographs and work safely.

It must be understood that the need to obtain consent for the use of images, is to be applied to adults as well as children.

Using images of children supplied by a third party

Statement of intent

It must be recognised that photographs and other images are subject to copyright, which will generally rest with the photographer. Prior permission must therefore be obtained before such images are to be used.

Procedures

Before using any image supplied by a third party, it is to be ensured that the third party owns the copyright and that consent has been given in writing by the individual(s) concerned to use the image.

Where a third party provides such photographs / images, they will be obliged to confirm in writing that they have the express consent of the parent or carer to use the said image, where applicable.

Use of images of children by the media

Statement of intent

There may be occasions where the press are invited to a planned event to take photographs of the children and young people who are to take part. It should be noted that the press enjoy special rights under the Data Protection Act, which permit them to publish material for journalistic purposes.

Generally, parents and carers will take pride in 'press cuttings'. For the majority, this pride will often outweigh any fears about the image and / or information being subject to misuse. However, some parents may object to information about, and images of, their own children being published. As a result, it is to be ensured that parental / carer consent will be sought before the press is to be given any access to children and young people. Should a parent or carer choose not to give permission for their child to be photographed in such circumstances, this right must be observed at all times.

Procedures

The manner in which the press will use images is to be controlled through relevant industry codes of practice as well as the law. In this way a check is to be put on the potential improper use of images of children and young people by the press. Additional checks will however also be carried out by the Senior Designated Person for Safeguarding. This will ensure that broadcasters and press photographers are to be made aware of the sensitivity which must be considered in respect of detailed captioning, one to one interviews, and close up sports photography.

Where a press photographer is to be invited to celebrate an event, every effort will be made in advance to ensure that the newspaper's (or other relevant media) requirements are able to be met. Where, for example, a newspaper is to be invited to take photographs of children and young people, it is unacceptable for their names to be completely withheld. Newspapers will be very unlikely to print anonymous photographs. An agreement will therefore be sought between parents and carers and the press which will request that first names only will be published. Responsibility and liability however cannot be held for the actions of a third party organisation, should they choose not to abide by any such agreement once in place.

Consideration will therefore be given to the requirements of the press before any planned event. Parental / carer permission / opinion will be the key factor in making a decision as to whether the press will be invited or not. This may mean that only those children, whose parents or carers will be happy for photographs and names to be published, can be given the opportunity to be involved in such events.

Should it not be considered possible or appropriate to limit the children and young people who are to be photographed, for example, because a specific group of individuals are to have achieved something special (and parental permission regarding the publication of first names is to be withheld by one or more of the group) efforts will be made to negotiate a revised agreement with the press which must be deemed acceptable to all parties. Should it not be possible for such an agreement to be reached, the option of newspaper publicity will have to be forgone.

The identity of any press representative will be verified. Access will only be permitted where the event is to be planned, and where press are to be specifically invited to attend. No authorisation will be given to unscheduled visits by the press under any circumstances. In the event that the press should turn up uninvited, for reasons beyond the control of the setting, every reasonable effort will be made to ensure that children and young people and parents and carers are protected from any press intrusion.

Every effort will be made to ensure the press abide by any specific guidelines should they be requested by the setting. No responsibility or liability however can be claimed for situations beyond reasonable control, and where the setting is to be considered to have acted in good faith.

Use of a professional photographer

Statement of intent

It will be ensured that any professional photographer who is to be engaged to record any events will be prepared to work according to the terms of this policy document and the following guidelines:

- In the context of data protection legislation, the photographer will be considered a 'data processor' and any agreement with them will be in accordance with the Data Protection Act 1998.
- Photographers will only be used where they will guarantee to act appropriately to prevent unauthorised or unlawful processing of images; and will insure against accidental loss or destruction of, or damage to, personal data.

Procedures

Photographers will be asked to sign an agreement which will aim to ensure:

- compliance with the Data Protection Act 1998.
- images are only to be used for a specified purpose and will not be used in any other context.
- images will not be disclosed to any third party unless it is to be a specific requirement to do so in order to fulfil the requirements of the agreement. Such use will also be subject to parental / carer permission.

Only reputable photography agencies and / or professional photographers will be used. Evidence of such authenticity will be required.

Details of any checks regarding suitability, which are to include evidence of Disclosure and Barring Service checks, will be requested. Photographic identity will be checked on arrival. Should there be any concerns in respect of the authenticity of any photographer, entry will be refused. Such concerns will be reported as is to be deemed appropriate.

Photographers are to be treated as any other visitor. As such, appropriate levels of supervision will be in place at all times. This will ensure that no unsupervised access to children and young people will be given.

Children photographing each other

Statement of intent

Children may on occasion be given the opportunity to photograph each other and their surroundings. This practice will often occur during off-site activities and for most children it will be normal practice to take photographs to record a trip or event. Children may also be given access to cameras within the setting environment to support their learning and development needs. These activities will be encouraged in a safe and enabling environment.
The children's camera are a part of ICT education in line with the EYFS and do not leave the pre-school site.

Procedures

Early years practitioners and their managers will be required to discuss and agree some age appropriate acceptable use rules with children and young people regarding the appropriate use of cameras.

Nevertheless there may be occasions where children will take inappropriate images, including photographs which may show friends and other children in a state of undress. This practice will be discouraged, and parents will also be advised to monitor their child's use of cameras within the home and social environment.

The right of parents and carers to take photographs and videos

Statement of intent

Parents and carers will not be covered by the Data Protection Act 1998 if they are to take photographs or make a video recording for their own private use. The Act will therefore not prevent parents and carers from taking photographs or making video recordings of their own children within the setting environment, for example, during nativity plays.

The right to refuse parents and carers the opportunity to take photographs and make videos is however to be reserved on health and safety grounds. This right will be implemented should it be deemed appropriate. For example, if an excessive use of flashlights and / or bulky and noisy equipment are to be considered a potential health and safety risk.

Procedures

Parents and carers will be required to complete a Photography Request Form should they wish to take or make any recordings within the setting environment. Authorised use will only be permitted on agreed dates and times, and within designated areas of the setting.

Before a photography request can be authorised, consent will need to be obtained from all parents and carers of other children who may be captured in any photograph or video. Should it not be possible, to gain consent from the parents and carers of all children who may be implicated, there will be no option but to refuse an open request to take or make images. Consideration will however be given to organising a one-off photograph opportunity which will only involve those children for who consent has been obtained.

Parents and carers will only be permitted to make recordings or take photographs of any event for their own personal use. The use of such images and recordings for any other purpose, without express permission, will be a breach of the Data Protection Act 1998.
Parents and carers who are to be authorised to use photographic equipment must be encouraged to be mindful of others when making and taking such images. This will be to ensure minimum disruption to other parents and carers during any event or production. Care must be taken to ensure the view of others will not be obscured and intrusive photography or filming must be avoided at all times. The right to withdraw consent will be maintained and any images or filming must be open to scrutiny at any time.

Every effort must be made to ensure that individuals with no connection to the early years setting are to be given no opportunity to film covertly. Early years practitioners and their managers are to have the authority to question anybody they do not recognise (subject to their own safety being ensured) should they be observed using any photographic equipment at events and productions or within the general vicinity. Care will be taken at all times to prevent any opportunist photography or filming taking place.

Web-cams

Statement of intent

Parental consent must be obtained before web-cams will be used within the setting environment. Before seeking such consent, full details of why a web-cam is to be used will be provided. This will also include information on the use of images, who is to be given authority to view them, and the security measures which will be implemented to prevent unauthorised access.

Procedures

All areas which are to be covered by a web-cam must be well signposted, and notifications are to be displayed so that individuals will be advised before entering such vicinity.

Consultation is to be carried out with children, young people, parents and carers, practitioners and their managers to determine if they are to be in agreement to being filmed. Written consent is to be obtained from all parents and carers.

Should a web-cam be used within the early years setting, it must be ensured that the manufacturer's instructions and data protection and information sharing guidelines are to be followed at all times. This is to include the appropriate storage and disposal of all recordings.

Mobile phones

The Mobile Phone Policy is to be referred to.

Use of internet / intranet sites

The Internet Policy is to be referred to.

Website

Statement of intent

It is to be understood that the posting of images on websites may raise particular issues and concerns.

It must be recognised that there will be a risk that such images could be subject to manipulation and circulation without consent or even knowledge. The risk that children and young people could be exploited in some way after having their image displayed must also be acknowledged.

However, the value offered by websites also needs to be appreciated. They are to give children and young people extensive creative opportunities for design and development. For some children and young people this will provide a medium which will best suit their individual learning style. This will give them the opportunity to succeed and excel. Access to moderated websites is therefore to be encouraged in a safe and age-appropriate environment.

Procedures

Displaying images of children and young people on the setting's external website is to be avoided, wherever possible. Should consideration be given to using images for display, explicit consent from the parent or carer will be required. Any images used will be copy-protected, include a watermark, and / or will be published in low definition to reduce the potential for misuse. Under no circumstances will a child's photo be published on any insecure social networking sites, such as Facebook or Bebo.
There will be no names given with any photo displayed on our website. The setting will ensure that a child cannot be identified by having a photo and a name of that child.

The use of secure learning platforms such as 'Merlin' is however to be promoted. Photographs of children and young people can be securely posted and such use is to be encouraged. Parent or carer consent will be requested before any images are uploaded.

A photo of a child will not be displayed on the website if parental/carer consent is not given.

Learning journeys

Statement of intent

Under the Early Years Foundation Stage, early years practitioners and their managers are to be encouraged 'to track children's progress and have a system for channelling the wealth of information gathered about individual children into a manageable summary. Detailed individual observations of self-initiated activity in a particular context, photos and special moments contained in a child's portfolio all document the child's unique learning journey'. (Progress Matters, National Strategies). Such portfolios will often be known as learning journeys and these are to be used to document and monitor the individual learning and development progress of each child in the early year's age group (birth to five years).

On line learning journeys

We use online learning journeys at Greenshoots and have strict guidelines for staff in our tapestry policy. Refer to tapestry policy.

Procedures

Tapestry is securely used by all members of staff who have access to it. All staff are given a copy of the Tapestry policy.

Staff and parents have secure passwords in order to access Tapestry.

Under no circumstances are staff allowed to access Tapestry on their own personal equipment or at home. Only the managers know the main signing in password for Tapestry.
Tapestry will be monitored by the managers and images will be checked and monitored on a daily basis.

The information contained within each learning journey is to relate to an individual, identifiable child; therefore it is to be treated as personal data. This means that such information is to be stored securely when not in use. The aim will be to avoid unauthorised access to potentially sensitive data.

A code of practice trust statement is to be advocated to protect and promote the welfare and individual rights of children and young people. Details of this code of practice will therefore be included on a Learning Journey Consent form.

Consent must be obtained from parents and carers should their child be photographed amongst a group of children; and where consideration is to be given to including that image in a learning journey belonging to another child. It will be anticipated that this will be a regular occurrence, as group activity shots are to be encouraged.

Where possible, therefore, 'blanket' consent will be requested from parents and carers for group images to be included in the learning journeys of other children. Parents and carers must be given the option to view any images before they are to be included in any learning journey, should they request to do so. Parents and carers will also be permitted to restrict their consent. This may mean that group images can only be included in specified learning journeys, for example, those which are to belong to close friends. Should it not be possible to obtain consent, the relevant image must not be shared across learning journeys of other children.

Individual learning journeys, although to be constructed by early year's practitioners and their managers, are to be provided for the benefits of the individual child and their parents or carers. Parents and carers are therefore to be given the responsibility for choosing what to do with any personal data contained in the learning journey, once it is to be in their possession. However parents must be made aware that they are not permitted to 'publicise' another child or young person without the express agreement of the parent or carer concerned. Parents and carers must therefore be reminded that they must not share, distribute or display said images without relevant authorisation and consent from the parents and carers of all children and young people captured in any of the photographs.

Early years practitioners training portfolios

Statement of intent

During training, early years practitioners may be required to compile portfolios which will be used to document and evidence their own learning. Part of this documentation is likely to include images of the early years practitioner working alongside children and young people participating in various activities. Should such evidence be required, parent or carer consent will be requested.

The Senior Designated Person for Safeguarding is to have a duty of care to ensure early years practitioners are to act responsibly in compiling the images to be included in training portfolios. Early years practitioners will therefore be monitored in their taking, making and use of such images. All images will be subject to scrutiny and regular audits will be carried out to ensure all relevant policies and procedures are to be adhered to.

Procedures

The Senior Designated Person for Safeguarding will oversee the compilation of images which are to be used by early years practitioners when completing training portfolios. Any images which are to be deemed unsuitable for any reason will not be included.

Should images be considered inappropriate, the Senior Designated Person for Safeguarding will ensure the ICT Misuse Policy is to be applied.

Displaying images

Statement of intent

It must be ensured that still images (including those which are to be displayed in digital photo frames) and video clips are to depict children and young people in an appropriate way. The identity of individual children should also be protected. Particular caution should be taken where images are to be displayed in a public place. (The definition of a public place is to include any areas where parents and carers, members of the public and visitors are to be given access). Images of children displayed in the setting will not have a name with it. A child's identify cannot be recognised by a name and a picture.

Procedures

Digital photo frames or television screens are to be used to display slideshows of children and young people at play. Specific consent must be obtained from parents and carers to allow images to be used in such a way.

Increased sensitivity and security procedures are to be observed when digital photo frames are to be used. The careful positioning of such frames should be considered, as they are often to be displayed in the most public areas of the setting, such as the reception.

Documentation panels are to be encouraged and will include, for example, photographs, observation notes and transcripts of children's communications. Information included may be personal to an individual child and should not be considered for public information. Care should therefore be taken to ensure individual children and young people will not be identifiable. Children and young people should not be named if their photograph is to be displayed; and transcripts of communications (which may add to a child's personal profile) are to be placed randomly across the documentation panel. Transcripts are not to be attributed to individual children and young people. Should observation notes relating to individual children be displayed, confidentially must be observed at all times. Where necessary, this is to involve the removal of personal information. Alternatively a cover sheet will be placed over the top of the observation.

Where photographs are to be displayed in any context, the use of close up images of children and young people (particularly where they are to have been photographed against a blank background) should be avoided. Photographs of children and young people must be purposeful and show them in an appropriate context.

Storage and disposal

Statement of intent

Images are to be stored and disposed of securely. The aim will be to prevent unauthorised access, ensure confidentiality and protect identity. All images are to be stored and disposed of in line with the Data Protection Act 1998.

Procedure

Images will not be kept for longer than is to be considered necessary. The Senior Designated Person for Safeguarding is to ensure all photographs are to be permanently wiped from memory cards, computer hard and portable drives or other relevant devices once the images will no longer be of use.

Should images need to be kept for a short period of time, they must be protectively stored and password protected on the computer hard drive or other appropriate storage device. Such equipment will be stored securely and access will be restricted.

Photographs will only be stored on portable storage devices for a temporary period. Express permission must be obtained from the Senior Designated Person for Safeguarding and effective security measures must be in place.

Security measures are to be the same that apply to any personal data and means that such data:
- Must be classified as protected, restricted or confidential.
- Must be marked for relevant disposal.
- Will not be removed from the site physically or electronically without suitable encryption (password protected is not enough by law). Suitable encryption software is to be found at: http://www.truecrypt.org/downloads or http://www.axantum.com/AxCrypt/Downloads.html

All images, including those held within learning journeys will remain on site at all times, unless prior explicit consent has been given by both the Senior Designated Person for Safeguarding and the parent or carer of any child or young person captured in any photograph. Should permission be given to take images off site, all relevant details are to be recorded, for example who, what, when and why.
Photographs must be disposed of should they no longer be required. It must be ensured that they will be returned to the parent or carer, deleted and wiped or shredded as appropriate. Copies are not to be taken of any images without relevant authority and consent from the Senior Designated Person for Safeguarding and the parent or carer.

A record of all consent details are to be kept on file. Should permission be withdrawn at any time, all relevant images will be removed and disposed of. The record will be updated accordingly.

Security

Statement of intent

All images are to be handled as personal data and deemed to be of a sensitive and confidential nature. It is to be recognised that damage or distress could be caused if security is to be breached. The responsibility of being in a position of trust in handling such data must therefore be taken seriously.

The Senior Designated Person for Safeguarding is to be responsible for ensuring all information is handled appropriately and securely. Should there be any concerns over breaches of security, the Senior Designated Person for Safeguarding and / or the registered person will be required to undertake an investigation as is to be deemed appropriate. All such incidents are to be recorded and where necessary reported to the relevant authorities. Any actions which are to be identified as a result of any investigations must be implemented with immediate effect.

Procedures

Security procedures are to be monitored and reviewed at the end of every two month period.

Under the Data Protection Act 1998, reasonable steps must be taken to ensure the reliability and suitability of any individual who is to have access to personal data. Early years practitioners and their managers are therefore considered to be in a responsible position of trust.

To this effect, effective safer recruitment procedures are to be applied. Rigorous and regular checks are also to be undertaken to ensure the on-going suitability of all new and existing early years practitioners and their managers. All relevant checks must be completed before any new employee, volunteer or student is to be given access to children and / or their personal data.

All early years practitioners are to be required to follow confidentiality and information sharing procedures, which must be agreed to at the time of induction.

The following aspects of security are to be managed accordingly:

- Physical security – effective measures are to be put in place to ensure physical security and to Protect against theft, including that of laptops, computers, cameras, and any personal data, Including photographic images.
- Computer security – stringent measures are to be implemented to ensure computer security. Awareness will be raised in respect of technological advancements which could put online systems at risks. Security will be updated as and when it is to be required.

Security procedures are to be proportionate to the potential risks involved and must be subject to constant monitoring and review.

This policy was adopted on:

Signed on behalf of Laira Green Trust - Greenshoots Pre-school and Wraparound Care

Chairperson, Laira Green Trust:

Greenshoots Manager (Strategy and Support)

For the benefit of this policy Laira Green Trust – which is the governing body of Greenshoots Pre-school and Wraparound care is hereafter referred to as Greenshoots.

Mobile Phone Policy

Introduction

Mobile phone technology has become more sophisticated over recent years and will continue to evolve. Wireless connections in particular are to extend the capabilities of mobile phones further; which will allow access to new content and services, such as the internet, social networking sites and instant messaging. Many mobile phones offer camera, video and audio recording as standard.

Mobile phones, alongside other technologies aim to change the way we communicate. This speed of communication will often provide security and reassurance; however, as with any other form of technology there are to be associated risks. Children and young people must be encouraged to understand such risks to enable them to develop the appropriate strategies which will keep them safe.

As with online safety issues generally, risks to children and young people should be broadly categorised under the headings of:
• content
• contact
• conduct
• commerce.
These issues are to be managed by reducing availability, restricting access and increasing resilience.

This philosophy is to be applied to the use of mobile phones through the Mobile Phone Policy. Acceptable use and management of mobile phones is therefore to be agreed by all service users. There is to be a clear expectation that the personal use of mobile phones is to be limited to specific times and uses as to be agreed with the Senior Designated Person for Safeguarding. Any authorised use of mobile phones is to be monitored and recorded. Safe and secure storage facilities are to be made available to store personal belongings as necessary.

Under no circumstances are images, video or audio recordings to be made without prior explicit written consent by the Senior Designated Person for Safeguarding.

Aim

The aim of the Mobile Phone Policy is to protect children and young people from harm, by ensuring the appropriate management and use of mobile phones by all individuals who are to come into contact with the early years setting.

Children and young people are also to be empowered with the skills to manage the changes in technology in a safe and appropriate way; and to be alert to the potential risks of such use.

This is to be achieved through balancing protection and potential misuse. It is therefore to be recognised that alongside the potential risks, mobile phones continue to be effective communication tools. This in turn is to contribute to safeguarding practice and protection.

Scope

The Mobile Phone Policy will apply to all individuals who are to have access to and/or be users of personal and/or work-related mobile phones within the broadest context of the setting environment. This will include children and young people, parents and carers, early years practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not to be considered exhaustive.

Policy Statement

It is to be recognised that it is the enhanced functions of many mobile phones that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse are to include the taking and distribution of indecent images, exploitation and bullying.

It must be understood that should mobile phones be misused, there will be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to children and young people, so the needs and vulnerabilities of all must be respected and protected.

Mobile phones will also cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others.

It will often be very difficult to detect when mobile phones are present or being used. The use of all mobile phones needs to be effectively managed to ensure the potential for misuse is to be minimised.

Designated 'mobile use free' areas are to be situated within the early years setting, and signs to this effect are to be displayed throughout. The areas which should be considered most vulnerable include:
• sleep areas
• changing areas
• toilets
• bathrooms.

Code of conduct

A code of conduct is to be promoted with the aim of creating an informed workforce, who will work together to safeguard and promote positive outcomes for the children and young people in their care.

It is to be ensured that all practitioners and their managers will:
• be aware of the need to protect children from harm.
• have a clear understanding of what constitutes misuse.
• know how to minimise risk.
• be vigilant and alert to potential warning signs of misuse.
• avoid putting themselves into compromising situations which could be misinterpreted and lead to

potential allegations.
• understand the need for professional boundaries and clear guidance regarding acceptable use.
• be responsible for the self-moderation of their own behaviours.
• be aware of the importance of reporting concerns immediately.
It is to be recognised that studies consistently indicate that imposing rigid regulations and/or 'bans' on the actions of others are counterproductive and should be avoided. Such imposition will lead to a culture of suspicion, uncertainty and secrecy. An agreement of trust is therefore to be promoted regarding the carrying and use of mobile phones in the early years setting. This is to be agreed by all service users, including all children, young people and adults who are to come into contact with the early years setting.

Procedures

Under no circumstances will staff use their personal mobile phones around the setting where children are present. Mobile phones will be stored in the office or in the settings safe.
Mobile phones can be used by the staff on their breaks in the office or away from the setting when leaving the premises. The phone will remain in the staff member's bag until they have left the School premises.

Smart watches are the newest technology that we need to be aware of. They are considered by many as tiny smart phones on your wrist. They can be used to send and receive messages, emails, make phone calls and connect to social network sites. The latest versions of the smart watches also have the ability to take photographs as there are mini cameras built into the device. Like other computers, a smart watch may collect information from internal or external sensors. It may control, or retrieve data from, other instruments or computers. Smart watches must never be used to take videos or photographs of children.

Smart watches are treated the same as a mobile phone. It will be stored in the office or the setting's safe and can be accessed away from the children on breaks and when left the premises.

Clearly defined policies and procedures will aim to ensure effective safeguarding practices are in place to protect children from harm and exposure to behaviours associated with misuse. The need to ensure mobile phones will not cause unnecessary and/or unsafe disruptions and distractions in the workplace are also to be considered.

Acceptable use and management of mobile phones is to be agreed by all service users. There is to be a clear expectation, for example, that all personal use of mobile phones is to be limited to allocated lunch and/or tea breaks, unless it is to be otherwise agreed by the Senior Designated Person for Safeguarding. Such authorised use is to be monitored and recorded. Safe and secure storage facilities are to be made available to store personal belongings as necessary.

The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it is to be explicitly agreed otherwise by the Senior Designated Person for Safeguarding. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Senior Designated Person for Safeguarding is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

Practitioners and their managers are to be encouraged not to use their own personal mobile phones for contacting children and young people, parents and carers. If it is to be deemed necessary, it must be with the explicit written consent of both the Senior Designated Person for Safeguarding and the parent or carer; unless it is to be considered an emergency. Care is to be taken to ensure that work mobiles are not to be exploited in a similar way.

Children and young people are to be enabled to have access to their own personal mobile phones should they choose. This will be subject to signed agreement by the parent or carer. Safe management and acceptable use of such mobile phones is to be promoted and monitored.

Children and young people's mobile phones are to be switched off or to be set on silence during the course of the day, except where express signed permission is to be given to do otherwise.

All service users, including parents, carers, visitors and contractors should be respectfully advised that their mobile phones are not to be used in designated mobile use free areas. Should it be considered necessary for mobile phone calls and/or texts to be taken or made, efforts should be made to avoid any unnecessary disturbance or disruption to children and young people. No images, video or audio recordings are to be made without prior explicit written consent by the Senior Designated Person for Safeguarding.

All individuals who are to bring personal devices into the early years setting must ensure that they hold no inappropriate or illegal content.

Work mobile

The use of a designated work mobile is to be promoted as it is considered to be:
- an effective communication tool, enabling text, email messages and calls to be made and received.
- an essential part of the emergency toolkit which is to be taken on short trips and outings.
- a back-up facility should landline facilities be unavailable – or where contact needs to be made outside of operational hours.

Effective security procedures are to be put in place to safeguard against any potential misuse. Only authorised individuals are to have access to the work mobile, which is to be password protected, and to be stored securely when not in use. All use is to be recorded and monitored by the Senior Designated Person for Safeguarding.

Personal calls are not to be made on the work mobile phone, other than in circumstances to be agreed. Personal contact will be permitted to be made via the work mobile in the event of an emergency. All such communications are to be logged.

No images of children will be taken on the settings phone.

The work mobile phone is to be clearly labelled as such.

Driving

Practitioners and their managers who will be required to drive on behalf of the early years setting must ensure any work and/or personal mobile phones are to be switched off whilst driving.

Under no circumstances, when driving on behalf of the organisation, should practitioners and their managers make or take a phone call, text or use the enhanced functions of a mobile phone. This is also to apply to the use of hands-free and wireless connections, which are to be considered a distraction rather than a safer alternative.

Safe storage

A designated safe and secure area is to be made available to practitioners and their managers for the storage of personal belongings during the working day.

Practitioners and their managers should recognise that they are to leave any belongings in such storage areas at their own risk. It is recommended that should mobile phones be stored, they are to be security marked, password protected and insured. No liability for loss and/or damage is to be accepted.

Emergency contact

It is to be recognised that mobile phones provide direct contact to others, and will often provide necessary reassurances due to their ease of access, particularly at difficult times. Agreed acceptable use of mobile phones is to therefore be promoted. This is to afford practitioners and their managers peace of mind, by reducing stress and worry and is therefore to allow them to concentrate more fully on their work. Such use must be subject to management, monitoring and review. It is to be ensured that the landline telephone remains connected and operational at all times, except in circumstances beyond reasonable control. This means that the landline is to be available for emergency/urgent contact at all times.

The reliance on an answer phone is to be avoided unless the early years setting should be closed or where children are to be taken off the premises for a trip or outing. It must always be ensured that the answer phone is to be checked promptly on opening or return.

This policy was adopted on:

Signed on behalf of Laira Green Trust - Greenshoots Pre-school and Wraparound Care

Chairperson, Laira Green Trust:

Greenshoots Manager (Strategy and Support)

For the benefit of this policy Laira Green Trust – which is the governing body of Greenshoots Pre-school and Wraparound care is hereafter referred to as Greenshoots.

ICT Misuse Policy

Aim

The ICT (Information and Communication Technology) Misuse Policy will aim to ensure any allegation, which is to be made in respect of the intentional or unintentional misuse of any online technologies, is to be addressed to in a responsible and calm manner. This is to include any known or suspected breaches of the Acceptable Use Policy, Camera and Image Policy, Internet Policy and Mobile Phone Policy.

Allegations are to be dealt with promptly, sensitively and fairly in line with agreed procedures. The ICT Misuse Policy will also outline the sanctions that are to be applied should an incident occur.

The overall priority will be to ensure the safety and well-being of children and young people at all times. Should it be suspected at any stage that a child or young person may have been or is considered to be subject to abuse, the Safeguarding Policy and Procedures must be implemented with immediate effect. These procedures are also to be followed should an allegation of abuse be made against any employee, manager, volunteer or student. The Safeguarding Policy is to take precedence over all others, and referrals must be made to the appropriate agency as deemed necessary.

Scope

The ICT Misuse Policy will apply to all individuals who are to have access to and/or be users of work-related ICT systems. This will include children and young people, parents and carers, early years practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not to be considered exhaustive.

The policy will be implemented in respect of any potential breaches of the Acceptable Use Policy, Camera and Image Policy, Internet Policy and Mobile Phone Policy.

Responsibilities

The registered person and the Senior Designated Person for Safeguarding are to be responsible for ensuring that the procedures outlined herein will be followed. These procedures are to be considered should an allegation of misuse be made against a child, young person or adult.

Policy Statement

Clear and well-publicised policies and procedures which will influence practice, are to be considered the simplest and most effective way for the safe use of ICT to be upheld. Such policies and procedure should ensure the promotion of acceptable use and clearly define those behaviours which are not. The sanctions to be imposed in respect of any incidents of misuse should be identified.

It will be ensured that:
- relevant online safety policies and procedures will be fully implemented, monitored and reviewed. These policies and procedures are to be rigorous, manageable and reflective of practice; and are to be shared with all ICT users. The Senior Designated Person for Safeguarding will be responsible for the management of such policies.
- all ICT users are to be made aware of possible signs of potential misuse. Adults, in particular, will be responsible for observing practice and behaviours, so that any significant changes in such are to be identified at the earliest opportunity.
- all ICT users are to be made aware that the misuse of ICT and/or breaches of relevant policies and procedures are to be taken seriously. All ICT users are to be made aware of the potential sanctions that could be applied should such concerns be raised.
- effective reporting and whistle-blowing procedures are to be in place and promoted.

It is to be acknowledged, however, that no system or procedure can be considered 100 per cent safe, secure and fool-proof. It should therefore be accepted that the potential for ICT to be misused, whether intentionally or unintentionally will remain. The aim of the online safety policies will therefore be to minimise such opportunities and risk.

Procedures

General

All incidents are to be dealt with on an individual case by case basis, and an escalating tariff of agreed sanctions are to be put in place.

The context, intention and impact of each incident are to determine the response and actions to be taken. This will allow for a degree of flexibility as to how sanctions are to be applied, subject to the need for other policies to be implemented. For example, a series of minor incidents by one individual is likely to be treated differently than should it be deemed a one-off occurrence; similarly unintentional and intentional access to inappropriate websites are to instigate different levels of intervention and sanctions.

All online safety incidents are to be recorded and monitored, and any potential patterns in behaviours should be identified, to enable such issues to be addressed proactively and for protection to be afforded.

Misuse is to be categorised under the three headings of ‘minor incidents’, ‘significant incidents’ and ‘serious incidents’.

Minor incidents

The following procedure is to be followed should an incident be considered minor.
- The incident is to be reported to the Senior Designated Person for Safeguarding. A written incident record is to be made, and the situation is to be monitored.
- The context, intention and impact of such misuse must also be considered. Where deemed necessary the incident is to be escalated to a ‘significant’ or ‘serious’ level.
- Sanctions are to be applied in accordance with the Acceptable Use Policy.

Significant incidents

There will always be the possibility that through access to the internet children and young people may gain unintentional access to inappropriate materials. Such material may not be illegal, but is not to be considered suitable in a childcare environment and/or to be age appropriate.

An open reporting policy is to be in place which means that all inadvertent breaches and access to inappropriate materials must be reported. The non-reporting of such breaches are to result in the concern being escalated.

The following procedure is to be followed should an incident be considered significant.

- The incident is to be reported to the Senior Designated Person for Safeguarding. A written incident record is to be made.
- The context, intention and impact of such misuse must also be considered. Where deemed necessary the incident is to be escalated to a 'serious' level.
- Appropriate action is to be agreed between the Senior Designated Person for Safeguarding and the registered person.
- If the incident should relate to the inadvertent access to an inappropriate website, it is to be added to the banned or restricted list and filters are to be applied, where relevant.
- Sanctions are to be applied in accordance with the Acceptable Use Policy.
- In respect to misuse by children and young people, parents and carers are to be informed of the alleged incident and are to be advised of any actions to be taken as a result.

Serious incidents

It must be ensured that all serious incidents will be dealt with promptly and reported to the Senior Designated Person for Safeguarding and the registered person immediately.

The context, intention and impact of the alleged misuse must be considered.

Appropriate action is to be agreed between the Senior Designated Person for Safeguarding and the registered person. All details are to be accurately and legibly recorded. The reason why any decision is made will be also be noted.

Should it be considered at any stage that a child or young person is or has been subject to abuse of any form, the Safeguarding Policy will be implemented with immediate effect. A referral will be made to Children's Social Care and the Police, where applicable.

Should the incident relate to an allegation made against an employee, manager, volunteer or student; and there is a suggestion that a child or young person has been subject to any form of abuse, the Safeguarding Policy will again be implemented with immediate effect. The Local Authority Designated Officer must be contacted in the first instance in respect of any allegation made against an adult. The Police and Ofsted must also be contacted.

It is to be ensured that no internal investigation or interviews are to be carried out in respect of any allegations, unless it is to be explicitly requested otherwise by an investigating agency.

It is to be fully recognised that should allegations of abuse be made, Children's Social Care, the Police and/or the Local Authority Designated Officer will be the investigative bodies. It must therefore be ensured that no action is to be taken which could compromise any such investigations.

Where applicable, any hardware implicated in any potential investigations of misuse is to be secured, so that evidence can be preserved. This may include mobile phones, laptops, computers and portable media technology.

Internal disciplinary procedures must not be undertaken until investigations by the relevant agencies are to have been completed. Legal or human resources advice should be sought prior to carrying out any internal investigations and/or instigating high-level disciplinary procedures.

On completion of both internal and external investigations, or sooner where it is to be deemed appropriate, an online safety review is to be undertaken and policies and procedures are to be amended and updated as necessary. A consultation on any proposed revisions will be held with all ICT users as appropriate. Revised policies and procedures will be circulated as applicable.

By nature, serious incidents will most often involve illegal materials and activities, including the viewing, possession, taking, making and distribution of indecent images; bullying or harassment through the use of portable media devices, such as mobile phones or grooming. In such situations, these incidents may be instigated by a child, young person or adult.

The following incidents must always be reported to the Police, Children's Social Care, Local Authority Designated Officer and Ofsted:
• Discovery of indecent images of children and young people.
• Behaviour considered to be 'grooming'.
• Sending of obscene materials.
It should be understood, that by not reporting such incidents, an offence may be committed.

The seriousness of such allegations is to be fully recognised, and it must be ensured that all such incidents are to be reported to the Police immediately. No attempt is to be made to download, print or send any materials found. It should be understood that further offences could be committed by doing so.

Should potentially illegal material be discovered, as far as is reasonably practical, the equipment or materials found will not be touched. Computers or other devices will not be switched off unless it is authorised to do so by the Police. The focus must be on preventing further access to the illegal content by keeping other individuals out of the immediate area. Where necessary the monitor should be turned off (but the computer remain on).

Illegal material and activities which must be reported to the Internet Watch Foundation

A report is to be made to the Internet Watch Foundation[1] should potentially illegal material, including images of child abuse be discovered. If it is unclear whether the content is to be considered illegal or not, the concern will be reported as a matter of caution.

Should it be considered that materials are inappropriate but legal, such incidents will generally be dealt with through internal disciplinary procedures. Unless alleged criminal activity and/abuse is suspected, it will not normally be considered necessary to involve the Police or other agencies.

[1] IWF Internet Watch Foundation http://www.iwf.org.uk/reporting.htm

Media attention

It must be recognised that should a serious incident occur, it will most likely attract intense media interest and speculation. On such occasions, every possible attempt is to be made to ensure that children and young people, parents and carers are protected from such influences.

An agreed media strategy will be implemented, and statements must only be released by authorised personnel, in accordance with information sharing procedures. In all instances, the prime concern will be the safeguarding and welfare of the children, young people and their families. Advice will be taken from Services for Children and Young People where appropriate before any media engagement is to be undertaken.

This policy was adopted on:_____

Signed on behalf of Laira Green Trust - Greenshoots Pre-school and Wraparound Care

Chairperson, Laira Green Trust:

Greenshoots Manager (Strategy and Support):