Registered Charity No 1035670

Beckley Preschool
Online Safety Policies and Procedures

Contents

Summary

Beckley Pre-School wish to embrace the opportunities offered by advances in information and communications technology (ICT), while ensuring children are safeguarded and protected from potential harm. Rigorous online safety policies and procedures are essential to safeguarding children online.

Online Safety Pledge

Beckley Pre-School shows its commitment to online safety by pledging that:

1. The advantages and positive aspects of using digital technologies will be continually promoted among children.
2. Our Pre-School will have its own Acceptable Use Policy (AUP), which will be kept up to date as technology and its use develops, and which will be promoted among the Pre-School's staff, volunteers, children and parents/carers.
3. Our Designated Safeguarding Leads (DSL) are responsible for leading Online Safety in the settings. The DSL is conversant with children and young people's safe use of digital technologies and is responsible for ensuring that all necessary policies and procedures and safeguarding measures are in place.
4. An Acceptable Use Policy (AUP) will be promoted and made available to all those who use digital technologies, including children and their parents / carers.
5. Electronic safeguards, appropriate to the setting, will be put in place, in line with relevant national and local guidance and will be updated regularly. Reports generated from these will be used to confirm adherence to AUPs.
6. Children using digital technologies within this setting will be made aware of their online rights, and the potential risks and dangers.
7. Children will be equipped with the knowledge and encouraged to take responsibility for keeping themselves safe whilst using digital technologies.
8. Staff and volunteers will be made aware of safeguarding issues for children using digital technologies.
9. Procedures will be in place to ensure that action will be taken when there are concerns that these digital technologies have been used inappropriately.
10. Staff / volunteers, children and parents / carers will be made aware of how to report concerns / whom to speak to if they feel worried about, or are aware of, any online safety incidents.
11. All users will be consulted about, and involved in, the implementation of our pledge.

Acceptable Use Policy

Acceptable Use Rules for Children

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer.
- I will only use activities that an adult has told me or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Registered Charity No 1035670

Acceptable Use Agreement for Parents / Carers

Introduction and Letter

Dear Parent / Carer,

As part of their learning and development, your child will have the opportunity to access a wide range of digital technologies, including computers, games, consoles and cameras. We recognise the value of using these digital technologies and the potential risks involved. We therefore have rigorous online safety policies and procedures in place. Copies of our Online Safety Policies & Procedures are available in our Policies & Procedures Folder in the PreSchool and Nursery and on our website.

In order to support us further in developing your child's knowledge and understanding about online safety, please read the "Acceptable Use Rules for Children" below and discuss these with your child. We then ask that you 'sign' and return the attached slip. We understand that your child is too young to give informed consent on his / her own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful partnership.

Hopefully, you will also find these rules provide an opportunity for further conversations between you and your child about safe and appropriate use of the online and digital technologies, both within and beyond the early years setting environment, such as at home or at a friend's home.

Should you wish to discuss the matter further, please do not hesitate to contact the settings manager.

Registered Charity No 1035670

Acceptable use rules for children:

This is how we stay safe when we use computers:

 I will ask an adult if I want to use a computer.
 I will only use activities that an adult has told me or allowed me to use.
 I will take care of the computer and other equipment.
 I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
 I will tell an adult / a leader if I see something that upsets me on the screen.
 I know that if I break the rules I might not be allowed to use a computer.

As the parent / carer I have read and discussed the acceptable use rules above with my child and confirm that he / she has understood what the rules mean.

 I give permission for my child to use the online and digital technologies.
 I understand that the setting will take all reasonable precautions to ensure that my child will be safe when online, however, I understand that this manages risk but cannot eliminate it.
 I understand that the setting will take appropriate action in the event of any incidents.
 I will encourage my child to adopt safe use of online and digital technologies, both within and outside the setting

Name of child:

Name of parent / carer:

Signature:

Date:

Acceptable Use Agreement for Staff and Volunteers

The Acceptable Use Agreement is intended to support the online safety of the organisation and individual staff and volunteers through:

- Staff and volunteers acting responsibly to stay safer while online and being good role models for younger users.
- Effective systems being in place for the online safety of all users and the security of devices, systems, images, personal devices and data.
- Staff and volunteers being aware of how they can protect themselves from potential risks in their use of online technologies.

The term "professional" in this Agreement is used to describe the role of any member of staff, volunteer or responsible adult.

For my professional and personal safety I must understand that:

- I should ensure that my on-line activity does not compromise my professional responsibilities, nor bring the Pre-School into disrepute.
- My use of technology could be monitored.
- When communicating professionally I will use the technology provided by the PreSchool (e.g. email). These rules also apply when using the Pre-School's technology either at home or away from the Pre-School.
- Personal use of the Pre-School's technology is only acceptable with permission.

For the safety of others:

- I will not access, copy, remove or otherwise alter any other user's files, without authorisation.
- I will communicate with others in a professional manner.
- I will share other's personal data only with their permission.
- I understand that any images I publish will be with the owner's permission and follow the Pre-School's code of practice.
- Wherever possible I will use the Pre-School's equipment to record any digital and video images, unless I have permission to do otherwise

For the safety of the setting, I understand that:

- I will not try to access anything illegal, harmful or inappropriate.
- It is my responsibility to immediately report any illegal, harmful or inappropriate incident.
- I will not share my online personal information (e.g. social networking profiles) with the children in my care.

 I will not deliberately bypass any systems designed to keep the Pre-School safer.
 I will only transport, hold, disclose or share personal information about myself or others, as allowed by the Data Protection Policy of the setting (or other relevant policy). Where personal data is transferred externally, it must be encrypted.
 I understand that Data Protection Policy requires that any personal data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by the setting's policy to disclose such information to an appropriate authority.
 Personal passwords and those of other users should always be confidential.
 I will not download anything that I do not have the right to use.
 I will only use my personal device if I have permission and use it within the agreed rules.
 I will inform the appropriate person if I find any damage or faults with technology.
 I will not attempt to install programmes of any type on the devices belonging to the PreSchool, without permission.

I have read and understand the above and agree to use the setting's technology and my own devices when carrying out communications related to the Pre-School within these guidelines. I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

Staff / Volunteer name:

Signature:

Date:

Professional Conduct Agreement

We recognise that practitioners and their managers will use online and digital technologies in their personal and social lives. We do not seek to prevent any practitioner or manager from accessing online technologies however we do ask them to sign a voluntary Professional Conduct Agreement to ensure there is no confusion between their home and professional roles.

Practitioner name:

I agree that through my recreational use of social networking sites or other technologies that I will:

 Maintain professional standards to avoid bringing the Pre-School / Nursery into disrepute.
 Observe confidentiality and ensure any professional communications with children, parents or other professionals take place within clear and explicit professional boundaries.
 Take reasonable precautions to limit professional access to my social networks.
 Not request or respond to any personal information from a child, young person or client.
 Take reasonable steps to ensure that all communications are transparent and open to scrutiny. Report any known breaches of the above.

I understand that the completion of this form is optional. However, I voluntarily choose to complete it to safeguard my own professional reputation and that of Beckley Pre-School.

Signature:

Date:

Internet Policy

Introduction

 The internet is part of everyday life. Knowledge and experience of information and communication technology (ICT) should be considered as essential. Developmentally appropriate access to computers and the internet in the early years contributes significantly to children and young people's enjoyment of learning and development.
 Children and young people learn most effectively where they are given managed access to computers and control of their own learning experiences; however such use carries an element of risk. Early years practitioners, their managers and volunteers, alongside parents and carers, should make children and young people aware of the potential risks associated with online technologies. This empowers them with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.

Aim

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

Scope

 The Internet Policy applies to all individuals who have access to and / or are users of PreSchool related ICT systems. This includes children, parents and carers, early years practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not exhaustive.
 The Internet Policy applies to internet access through any medium, for example computers, mobile phones and gaming devices.

Responsibilities

 The Designated Safeguarding Lead is responsible for online safety, and manages the implementation of the Internet Policy.
The Designated Safeguarding Lead 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 aware of the procedures that must be followed in the event of a potentially unsafe or inappropriate online incident taking place.
 The recording, monitoring and filing of reports in the event of a potentially unsafe or inappropriate online incident. This should include the creation of an incident log which should be used to inform future online safety practice.

 All necessary actions are taken to minimise the risk of any identified unsafe or inappropriate online incidents reoccurring.
 Regular meetings 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 delivered and available to all early years practitioners, their managers and volunteers. This includes 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 Designated Safeguarding Lead, 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 an essential requirement for early years practitioners and their managers particularly where they have access to personal information. A list of authorised ICT users should be maintained, and access to sensitive and personal data should be restricted.
 Early years practitioners and their managers will be responsible for keeping their passwords secure and should ensure they are regularly updated. All ICT users should have strong passwords.
 Passwords should not be shared. Where children have their own passwords there should be the option to reset if lost or forgotten.
 Computers and laptops should be set to 'time-out' the current user session if they become idle for an identified period. All ICT users must 'log-out' of their accounts if they need to leave a computer unattended.
 If ICT users become aware that password security has been compromised or has been shared, either intentionally or unintentionally, the concern must be reported to the Designated Safeguarding Lead.

Internet Access

 Internet access for all ICT users should be managed and moderated in order to protect them from deliberate or unintentional misuse. Every reasonable precaution should 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 should be put in place where appropriate to 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 Policy and Agreements

 Effective audit, monitoring and review procedures

 Online activity should be monitored to ensure access is given to appropriate materials only.
 Computers and gaming devices should be sited in areas of high visibility which will enable children and adults to be closely supervised and their online use to be appropriately monitored.
 If a child accidentally accesses inappropriate material, it must be reported to an adult immediately. Appropriate action should be taken to hide or minimise the window. The computer should not be switched off, nor the page closed, in order to allow investigations to take place. All such incidents must be reported to the Designated Safeguarding Lead; who must ensure a report of the incident is made and that any further actions deemed necessary are taken.
 All early years practitioners and their managers should be made aware of the risks of connecting personal mobile devices to work-related ICT systems. Such use will be subject to explicit authorisation by the Designated Safeguarding Lead and will be stringently monitored.
 Should it be necessary, the download of files or programmes to any work-related system should be effectively managed and monitored.
 All users are responsible for reporting any concerns encountered using online technologies to the Designated Safeguarding Lead.

Online communications

 All official online communications should occur where possible through secure filtered email accounts. Settings should be aware that free, web-based email services are not considered secure for personal data and their use could put the setting at risk.

 All email correspondence should be subject to scrutiny and monitoring.

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

 It is strongly recommended that, where possible, a filtered server is used to monitor and prevent offensive material or spam. If, on rare occasions, security systems are not able to identify and remove such materials, the incident should be reported to the Designated Safeguarding Lead immediately.

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

 When using digital communications, staff and volunteers should:

  Only make contact with children and young people for professional reasons, and in accordance with the policies and professional guidance of the Pre-School.
  Not share any personal information with a child or young person e.g. should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.
  Not request, or respond to, any personal information from the child / young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
  Be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
  Ensure that all communications are transparent and open to scrutiny.
  Be careful in their communications with children so as to avoid any possible misinterpretation.
  Ensure that if they have a personal social networking profile, details are not shared with children and young people in their care (making every effort to keep personal and professional online lives separate).
  Not post information online that could bring the Pre-School into disrepute.
  Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.
  Only use (wherever possible) official equipment or systems to communicate with children.

 All ICT users are advised to exercise caution when opening emails where they do not know the sender or where the format looks suspicious and to avoid clicking on links or opening attachments in such emails.
 Children should be enabled to use online technologies as relevant to their age and development. Access to online communications should always be monitored by a supervising adult.

Managing mobile and emerging technologies

 Emerging technologies should be valued for the learning and development opportunities they 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 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 should be carefully managed within the early years setting, and children will only be permitted to use moderated child-focused sites under supervision. Early years practitioners and their managers are not permitted to use workrelated technologies for personal access to social networking sites.

 All ICT users should be encouraged to think carefully about the way information can be added and removed from websites by themselves and others. Moderated sites can afford maximum protection.

 Children should be taught to think carefully before placing images of themselves online and to be aware of details within images, such as badges, which could reveal personal and background information. Users should consider the risks of posting images online owing to the permanency of online material.

 Children must always be reminded not to give out or post personal details online, particularly information which could identify them or provide information that would contribute to their personal profile.

 Children should be educated on how to set and maintain web profiles to appropriate privacy levels and how to deny access to unknown individuals.

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

 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'. The use of such sites should 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 social networking sites must be avoided.

 Social networking sites and mobile technologies can be used for negative and anti-social purposes. Cyber bullying, for example, is unacceptable as is 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 Designated Safeguarding Lead.

Emerging technologies

 Emerging technologies can offer potential learning and development opportunities. Their use should be risk assessed before use by children. Where necessary, further training and guidance should be provided to ensure appropriate and safe use of any new technologies.

"Those adults who work with particularly vulnerable children need to be familiar with the broad spectrum of online risks facing children, and how they can support and empower children and young people to address them."
Professor Tanya Byron

Tapestry -Learning Journey

Dear Parent or Carer,

Your child's learning journey is used to reflect your child's time at our early years setting. It includes observations of your child at play, photographs and other information. The aim is to provide you with a continuous picture of your child's time at our setting. The learning journey, therefore, captures your child's own personal journey, based on their own individual starting point, interests and experiences.

We hope that you will be able to contribute information to this learning journey, perhaps by including some information and photographs which show what your child enjoys doing at home. This information will help us to ensure that the care, learning and development opportunities we offer your child compliment those you already offer.

Please remember however, that this learning journey contains personal data that relates not only to your child, but to other children who attend our early years setting. It is likely, for example, that some of the photographs enclosed will capture other children at play. Permission has therefore been obtained to include such information in your child's learning journey, however it must be remembered that such data is shared for your own personal use only. This means that information cannot be shared with others, or 'publicised' in any way, without the explicit consent of the parents or carers of those children who may be included. For example, such photographs cannot be displayed on a social networking site or displayed in a public place.

Child's name:

☐ I understand and agree with the Learning Journey Trust Statement.

☐ I understand that any data included within my child's learning journey which relates to another child, is for my information and personal use only.

☐ I will not seek to publicise, display or share such data with others, and will ensure the privacy of other families in doing so.

☐ I understand that my child's image may be used in group photographs which are included in other children's' learning journeys.

Parent/carer's name:

Signature (parent/carer):

Date:

Digital Image and Mobile Phone Policy

Introduction

 The use of digital images should be considered an essential and integral part of everyday life. As such, children, early years practitioners and their managers should be encouraged to use such technology in a positive and responsible way.
 It is recognised however, that digital technology has increased the potential for cameras and images 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 is managed sensitively and respectfully. A proactive and protective ethos should 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.

Aim

 The Digital Image and Mobile Phone Policy aims to ensure safer and appropriate use of cameras and images through agreed acceptable use procedures. This is in line with legislative requirements and aims to respect the rights of all individuals.

Scope

 The Digital Image and Mobile Phone Policy will apply to all individuals who have access to and / or are users of work-related photographic equipment. This will include children, parents and carers, early years practitioners and their managers, volunteers, students, committee members, visitors, contractors and community users. This list is not exhaustive.
 The Digital Image and Mobile Phone Policy applies to the use of any photographic equipment. This includes mobile phones and portable devices with inbuilt cameras as well as other forms of digital technology and resources for storing and printing images.

Responsibilities

 The Designated Safeguarding Lead (DSL) is responsible for ensuring the acceptable, safe use and storage of all camera technology and images. This includes the management, implementation, monitoring and review of the Digital Image and Mobile Phone Policy.
 Further details on the responsibilities of the Designated Safeguarding Lead, registered person, early years practitioners and their managers, parents and carers, children are to be found in the Acceptable Use Policy.

Legislative framework

 This policy complies with the requirements of the Data Protection Act 2018, General Data Protection Regulation (GDPR), 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 that meets the requirements 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

Code of conduct

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

 The use of cameras and other photographic equipment should be authorised by the Designated Safeguarding Lead. 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 should be designed for work-related purposes only. The use of personal photographic equipment should be avoided. If such use is allowed, authorisation must be obtained from the Designated Safeguarding Lead and all relevant details of use should be recorded.

 The transferring of images via unfiltered web mail or unprotected mobile media should be avoided. If remote access is given to the servers or systems where images are to be stored, access will only be given as authorised by the Designated Safeguarding Lead. Any personal data stored on servers outside of the UK must comply with standards designated by UK Data Protection Law.

 The Designated Safeguarding Lead 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 Designated Safeguarding Lead is responsible for ensuring the safe storage of all images, in accordance with the Digital Image and Mobile Phone Policy and the advice given by the UK Information Commissioners Office concerning the secure storage of personal data.

 Early years practitioners and their managers have a duty to report any concerns relating to potential misuse. Clear whistle-blowing procedures should 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 should be requested from the parent or carer on enrolment of their child. The purpose for taking any images should 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 no longer attends 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.

Procedures

 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

Statement of intent

 It is 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 should 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 firststep towards minimising any danger is 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; and therefore early years practitioners and managers should 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.
 Sensitivity must be shown to any child who appears uncomfortable; and the potential for misinterpretation must be recognised. Images should therefore not be taken of any child against their wishes.
 The taking or making of images of a child in a one to one situation with an adult must be avoided whenever possible; unless there is an agreed, specified reason for doing so. It must be recognised that the context of such situations is likely to be perceived as sensitive and the use of cameras will be seen as intrusive and open to misinterpretation. It should be recognised that this may leave both the adult and child in a vulnerable position and is therefore not accepted practice.
 Photographs should not be taken of any child if they suffer an injury; whether it is accidental or non-accidental. This will be deemed a misuse of power which will potentially cause the child to become distressed or to feel humiliated. Where necessary, medical help should be sought, and in the case of a suspected non-accidental injury, the Safeguarding Policy should be implemented with immediate effect.
 Images which may cause distress, upset or embarrassment must not be used.
 Images of children must only be taken when they are in full and suitable dress. In no circumstances are images to be taken of children in any state of undress. Should children be participating in sport activities, careful consideration must be given to the appropriateness of taking such images, in particular the angle at which shots are taken.
 The taking or making of images in sensitive areas of the early years setting, for example toilet cubicles and changing areas, are not permitted.
 It should be ensured that where a child or young person's name or any other identifying information appears in any caption or accompanying text alongside their photograph, for example on displays, documentation panels and name cards, particular care should be taken where such images are likely to be viewed by others, including the general public.
 Consideration should always be given where images are published. This will also include where parents are encouraged to be involved with online learning journeys. These systems must be designed to enable parents and carers to access their own child's photographs and work safely. Where parents take photographs of their child at a pre-school event, they should be made aware of expectations of how that image may be used. Images and videos should be used for their own or family's personal use only and parents / carers should be encouraged to:
 Think about privacy and who has the right to see their images, not only of their own child but of others.
 Think about the implications of sharing the images online. If the images are shared online then they must make sure they are limited to immediate family only and not made public.

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 who 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 should be ensured that parental / carer consent has been sought before the press is given any access to children. If a parent or carer chooses 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 controlled through relevant industry codes of practice as well as the law. In this way a check is put on the potential improper use of images of children and young people by the press. Additional checks should however also be carried out by the Designated Safeguarding Lead. This ensures that broadcasters and press photographers are made aware of the sensitivity in respect of detailed captioning, one to one interviews, and close up sports photography.
 Where a press photographer is invited to celebrate an event, every effort should 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 invited to take photographs of children, it is usual practice for names to be provided. Newspapers will be very unlikely to print anonymous photographs. You may request that only first names are used however responsibility and liability cannot be held for the actions of a third party organisation, should they choose not to abide by any of those requests.
 The identity of any press representative must always be verified. Access will only be permitted where the event is planned, and where press are 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 parents and carers are protected from any press intrusion.
 Every effort should be made to ensure that the press abide by any specific guidelines if requested by the setting. However, no responsibility or liability can be claimed for situations beyond reasonable control, and where the setting is considered to have acted in good faith.

Use of a professional photographer

Statement of intent

 It should be ensured that any professional photographer engaged to record any events is 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 2018 and GDPR.

 Photographers will only be used where they 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 should be expected to demonstrate that they have agreed to ensure:

- Compliance with the Data Protection Act 2018
- Images are only used for a specified purpose and will not be used in any other context
- Images are not disclosed to any third party unless it is 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

 Care should be taken when choosing photography agencies and / or professional photographers.

 Details of any checks regarding suitability, which may include evidence of Data Barring Service checks, will be requested. Photographic identity should be checked on arrival. If there are any concerns in respect of the authenticity of any photographer, entry will be refused. Such concerns should be reported.

 Photographers should be treated as any other visitor. As such, appropriate levels of supervision should be in place at all times. This will ensure that no unsupervised access to children is 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 should be encouraged in a safe and enabling environment.

Procedures

 Early years practitioners and their managers should discuss and agree some age appropriate acceptable use rules with children regarding the appropriate use of cameras.

Parents photographing their children

Statement of intent

 Parents and carers are not covered by the Data Protection Act 2018 and GDPR if they take photographs or make a video recording for their own private use. The Act does not prevent parents and carers 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 reserved.

Procedures

 Parents and carers should complete a Photography Acceptable Use Agreement if 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.
 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 and without express permission should not be allowed.
 Parents or carers who are authorised to use photographic equipment should be encouraged to be mindful of others when making and taking such images. This ensures minimum disruption to other parents and carers during any event or production. The right to withdraw consent will be maintained and any images or filming must be open to scrutiny at any time.

Closed circuit television (CCTV)

Statement of intent

 CCTV may be used for the following purposes:
  To control access
  To monitor security
  For site management, for example monitoring incorrect parking, manoeuvring vehicles and delivery arrivals
  For monitoring purposes, particularly within the building, in corridors and areas out of sight or not frequently trafficked by early years practitioners, for example in the vicinity of toilets (but not in toilet cubicles)
  For general and focussed observations of children, early years practitioners and their managers
  To act as an effective deterrent to prevent crime and to discourage trespass

Procedures

 All areas which are covered by CCTV must be well signposted, and notifications should be displayed so that individuals are advised before entering such vicinity.
 If CCTV is used within the early years setting, the manufacturer's instructions, data protection and information sharing guidelines should be followed at all times. This should include the appropriate storage and disposal of all recordings.

 Recordings should be retained for a limited time period only and for no longer than their intended purpose. This will generally be a maximum of no more than 30 days. All recordings should be erased before disposal.
 Regular auditing of any stored images should be undertaken by the Designated Safeguarding Lead.
 Every effort will be made to avoid inadvertently taking inappropriate images and therefore cameras will be placed and positioned sensitively. No cameras should be pointed directly at toilet cubicles or any other sensitive areas within the setting environment.
 Images taken outside of operational hours should be erased in accordance with the procedures previously identified.

Web-cams

Statement of intent

 Web-cam on the setting computer is disabled and covered over and is therefore not in use at all.

Procedures

 The regulations which apply to web-cams regarding signage should be the same as for CCTV.
 If filming takes place, children, young people, parents and carers, practitioners and their managers should be consulted. Written consent should be obtained from all parents and carers.
 The details for the storage and disposal of recordings should be the same as for CCTV.

Mobile Phones

Statement of Intent

 The aim of the Digital Image and Mobile Phone Policy is to protect children from harm, by ensuring the appropriate management and use of images captured on mobile phones by all individuals who come into contact with the early years setting.
 Children should also 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 should be achieved through balancing protection and potential misuse. Alongside the potential risks, mobile phones continue to be effective communication tools. This in turn contributes to safeguarding practice and protection.

Work Mobile

 The use of a designated work mobile should be promoted as:
  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 should be put in place to safeguard against potential misuse. Only authorised individuals should have access to the work mobile, which should be security protected, and stored securely when not in use.
 Personal calls should not be made on the work mobile phone, other than in circumstances to be agreed. Personal contact may be permitted via the work mobile in the event of an emergency. All such communications should be logged.
 The work mobile phone is to be clearly labelled as such.

Driving

 Practitioners and their managers who are required to drive on behalf of the early years setting must ensure any work and / or personal mobile phones are switched off whilst driving.
 When driving on behalf of the setting, practitioners and their manager should not make or take a phone call, text or use the enhanced functions of a mobile phone. This also applies to the use of hands-free and wireless connections, which can be a distraction rather than a safer alternative.

Use of internet / intranet sites Refer to the Internet Policy guidance.

Website

Statement of intent

 The posing of images on websites may raise particular issues and concerns.
 There is a risk that such images could be subject to manipulation and circulation without consent or even knowledge. The risk that children could be exploited in some way after having their image displayed should also be acknowledged.

Procedures

 Displaying images of children and young people on the setting's external website should be avoided wherever possible. If images are to be displayed, explicit consent from the parent or carer is required. Under no circumstances should a child's photo be published on any insecure social networking sites, such as Facebook, Bebo, Instagram, Twitter etc.
 The Pre-School uses a secure online learning system . Photographs of children can be securely posted. Uploading of images to this system is covered by the Photography Acceptable Use Agreement.

Tapestry - Learning journeys

Statement of intent

 Under the Early Years Foundation Stage, practitioners and their managers are 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 activity in a particular context, photos and special moments contained in a child's portfolio all document the child's unique learning journey, this is shown on the Tapestry we use. Such portfolios are known as learning journeys and these are used to document and monitor the individual learning and development progress of each child in the early years age group (birth to five years).

Procedures

 The information contained within each learning journey on Tapestry relates to an individual, identifiable child; therefore it should be treated as personal data. This means that such information should be stored securely when not in use. The aim is to avoid unauthorised access to potentially sensitive data.
 A code of practice trust statement should 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 in a Tapestry - Learning Journey Statement. It must be displayed on the front cover of all hard copy individual learning journeys.
 Consent must be obtained from parents and carers if their child is photographed amongst a group of children; and where the image is included in a learning journey belonging to another child.
 Where possible, therefore, 'blanket' consent should be requested from parents and carers for group images to be included in the learning journeys of other children. Parents and carers should 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 belong to close friends. If it is not possible to obtain consent, the relevant image should not be shared across the learning journeys of other children.
 Individual learning journeys, constructed by early years practitioners and their managers, are provided for the benefits of the individual child and their parents or carers. Parents and carers should therefore be given the responsibility for choosing what to do with any personal data contained in the learning journey, once it is 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 those images without relevant authorisation and consent from the parent and carers of all children captured in any of the photographs.

Early years practitioners' training portfolios

Statement of intent

 Under the Early Years Foundation Stage, practitioners and their managers are 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 activity in a particular context, photos and special moments contained in a child's portfolio all document the child's unique learning journey'. Such portfolios are known as learning journeys and these are used to document and monitor the individual learning and development progress of each child in the early years age group (birth to five years).

Procedures

 The information contained within each learning journey relates to an individual, identifiable child; therefore it should be treated as personal data. This means that such information should be stored securely when not in use. The aim is to avoid unauthorised access to potentially sensitive data.
 Consent must be obtained from parents and carers if their child is photographed amongst a group of children; and where the image is included in a learning journey belonging to another child.
 Where possible, therefore, 'blanket' consent should be requested from parents and carers for group images to be included in the learning journeys of other children. Parents andcarers should 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 belong to close friends. If it is not possible to obtain consent, the relevant image should not be shared across the learning journeys of other children.
 Individual learning journeys, constructed by early years practitioners and their managers, are provided for the benefits of the individual child and their parents or carers. Parents and carers should therefore be given the responsibility for choosing what to do with any personal data contained in the learning journey, once it is 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 those images without relevant authorisation and consent from the parent and carers of all children 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 participating in various activities.

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

Procedures

 The Designated Safeguarding Lead should oversee the compilation of images which are used by early years practitioners when completing training portfolios. Any images which are deemed unsuitable for any reason should not be included.
 If images are considered inappropriate, the Designated Safeguarding Lead should ensure the ICT Misuse Policy is applied.

Displaying images

Statement of intent

 It should be ensured that still images (including those which are displayed in digital photo frames) and video clips depict children in an appropriate way. The identity of individual children should also be protected. Particular caution should be taken where images are displayed in a public place. (The definition of a public place includes any areas where parents and carers, members of the public and visitors are given access

Procedures

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

Storage and disposal

Statement of intent

 Images should be stored and disposed of securely. The aim is to prevent unauthorised access, ensure confidentiality and protect identity. All images should be stored and disposed of in line with the Data Protection Act 2018 and GDPR.

Procedure

 Images should not be kept for longer than necessary. The Designated Safeguarding Lead should ensure that all photographs are permanently wiped from memory cards, computer hard drives, portable drives or other relevant devices once the images are no longer of use.
 If images need to be kept for a short period of time, they must be protectively stored on the computer hard drive or other appropriate storage device. Such equipment should be stored securely and access restricted.

 Photographs should not be stored on portable storage devices for any longer than is necessary.
 Security measures should be the same that apply to any personal data.
 All images, including those held within learning journeys should remain on site at all times, unless prior explicit consent has been given by the Designated Safeguarding Lead.
 Photographs should be disposed of when no longer required. They should be returned to the parent or carer, deleted and wiped or shredded as appropriate. Copies should not be taken of any images without relevant authority and consent from the Designated Safeguarding Lead and the parent or carer.
 A record of all consent details should be kept on file. If permission is withdrawn at any time, all relevant images should be removed and disposed of. The record should be updated accordingly.

Security

Statement of intent

 All images should be handled as personal data and deemed to be of a sensitive and confidential nature. It should be recognised that damage or distress could be caused if security is breached.
 The Designated Safeguarding Lead is responsible for ensuring that all information is handled appropriately and securely. If there are any concerns over breaches of security, the Designated Safeguarding Lead and / or the registered person are required to take action as appropriate. All such incidents should be recorded, reported and acted upon.

Procedures

 Security procedures should be monitored and reviewed regularly.
 Under the Data Protection Act of 2018 and GDPR, reasonable steps must be taken to ensure the reliability and suitability of any individual who has access to personal data.
 To this effect, effective safer recruitment procedures should be applied. Rigorous and regular checks should also 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 given access to children and / or their personal data.
 All early years practitioners are 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 should 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.
 Digital security – stringent measures should be implemented to ensure digital security. Awareness should be raised in respect of technological advancements which could put online systems at risk. Security should be updated as and when required.
 Security procedures should be proportionate to the potential risks involved and must be subject to constant monitoring and review.

Safe Storage

 A designated safe and secure area should 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 any belongings left in such storage areas are left at their owner's risk. It is recommended that if mobile phones are stored, they should be security marked, password protected and insured. No liability for loss and / or damage can be accepted.

Image Consent Letter and Form

Dear Parent/ Carer,

This letter explains why we will need to ask for consent before we are able to take photographs of your child during their time at Peasmarsh Flying Start Pre-School.

Generally, photographs are a source of pleasure and pride. We believe that the taking and use of photographs can enhance the self-esteem of children and their families and therefore is something to be welcomed and appreciated.

We may take photographs for a number of reasons whilst your child is with us, including to:

- document what they enjoy doing
- record their learning and development progress
- display in learning journeys and / or document panels
- record special events and achievements

We will also encourage children to be active learners, and to become involved in using cameras themselves by taking photos of their surroundings, activities and of each other.

We do however recognise that with the increased use of technologies, particularly digitally and online, the potential for misuse has become greater and we understand that this can give rise to concern. We will therefore endeavour to put effective safeguards in place to protect children by minimising risk. We will seek to protect children's identity and to limit opportunities for the taking, making and distribution of inappropriate images.

We often stage events for children to which parents are invited. Photographs of setting productions are ones which parents / carers tend to treasure. We will always try our best to allow parents / carers to use cameras at such events (on condition that they have signed the Acceptable Use Agreement).

Occasionally, we may invite the media into our early years setting to take photographs or film footage for publicity purposes and to record any special events. We will notify you of such occasions, and will seek specific permission for photographs to be taken, and potentially published at such times.

We are mindful of the fact that for some families, there may be reasons why protecting a child's identity is a matter of particular anxiety, and if you have special circumstances either now, or at any time in the future which would affect or change your position regarding consent, please let us know immediately in writing.

To comply with the Data Protection Act 2018 and GDPR, we need your permission before photographs and
recording of your child are made.
Please complete as appropriate.

Child's name:

☐ I consent to photographs of my child being taken by authorised personnel representing Beckley Pre-School and Northiam Nursery.
☐ I consent to any resulting images being displayed on walls or in digital photo frames within the Pre-School building where they may be visible at times to the general public or anywhere which could be defined as a 'public place'.
☐ I consent to any resulting images being used within the Individual Learning Journey of my child.
☐ I also consent to images of my child being used within the Individual Learning Journey of other children within the setting.
☐ I consent to my child's image being used on the Pre-School website, in publicity materials or in the media.
☐ I understand that I can withdraw my consent, or can request to see images taken at any time.
☐ I have discussed the policy with my child, and she / he is happy to be photographed, although I understand that at any time should she / he refuse or become upset, no photographs will be taken.

Parent/carer's name:

Signature
(parent/carer):

Date:

This form is valid for the duration of your child's time at our early years setting and for five years afterward. The consent will automatically expire after this time. It is your responsibility to
let us know in writing, if you want to withdraw or change your consent at any time.

Photography Acceptable Use Agreement

We recognise that parents and carers are likely to want to record early years setting productions or special events, and families will value the memories evoked from such images for years to come.
We request that parents and carers sign an Acceptable Use Agreement to cover the taking and use of such images, to ensure that the requirements of the Data Protection Act 2018 and GDPR are adhered to and the wishes of other parents / carers are respected.

I agree to:
☐ Use recording / photography only in the designated areas agreed
☐ Use recording / photography equipment on the agreed date and time only
☐ Respect the rights of other parents, and will not attempt to make any recordings if full parental consent cannot be obtained
☐ Stand to the rear of the designated area to avoid obstructing the view of others
☐ Avoid taking unnecessary close-ups of individual children (other than my own child)
☐ Stop recording / taking photos on the request of any staff member
☐ Ensure any photographs or videos taken are for my personal use only
☐ Not sell, publish or display such images in any form, including uploading of photos on to the internet, in line with Data Protection guidelines

Name of child:

Parent/carer's name:

Signature
(parent/carer):

Date:

Beckley Preschool

ICT Misuse Policy

Introduction

It is recognised that as digital technology has developed, so has the potential for misuse and the risks to children and young people. It must be acknowledged that technology itself will not present the greatest risks but the behaviours of individuals using such equipment. If it is suspected at any stage that a child or young person may have been or is considered to be subject to abuse, the Child Protection and Safeguarding Policy and Procedures should be implemented with immediate effect. These procedures should also be followed if an allegation of abuse is made against any employee, manager, volunteer or student. The Child Protection and Safeguarding Policy should take precedence over all others, and referrals should be made to the appropriate agency as deemed necessary.

Aim

The ICT (Information and Communication Technology) Misuse Policy aims to ensure that any allegation, which is made in respect of the intentional or unintentional misuse of any online technologies, is addressed in a responsible and calm manner. This includes any known or suspected breaches of the Acceptable Use Policy, Camera and Image Policy, Internet Policy and Mobile Phone Policy.
Allegations must be dealt with promptly, sensitively and fairly in line with agreed procedures. The ICT Misuse Policy should also outline the sanctions that are applied if an incident occurs.

Scope

The ICT Misuse Policy applies to all individuals who have access to and / or are users of workrelated ICT systems. This includes 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 exhaustive.
The policy should be implemented in respect of any potential breaches of the Acceptable Use Policy, Digital Image and Mobile Phone Policy and Internet Policy.

Responsibilities

The registered person and the Designated Safeguarding Lead are responsible for ensuring that the procedures outlined in this policy are followed. These procedures should be followed if an allegation of misuse is made against a child, young person or adult.

Policy Statement

Clear and well-publicised policies and procedures which will influence practice are the simplest and most effective way for the safe use of ICT to be upheld. Such policies and procedure shouldensure 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 is important that:
 Relevant online safety policies and procedures are fully implemented, monitored and reviewed. These policies and procedures should be rigorous, manageable and reflective of practice and should be shared with all ICT users. The Designated Safeguarding Lead is responsible for the management of such policies.

 All ICT users should be made aware of possible signs of potential misuse. Adults, in particular, are responsible for observing practice and behaviours, so that any significant changes are identified at the earliest opportunity.

 All ICT users should be made aware that the misuse of ICT and / or breaches of relevant policies and procedures are taken seriously, and that potential sanctions could be applied should such concerns be raised.

 Effective reporting and whistle-blowing procedures should be in place and promoted.
It should be acknowledged, however, that no system or procedure can be considered completely 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 is therefore to minimise such opportunities and risk.

Procedures

General
All incidents should be dealt with on an individual case by case basis, and an escalating tariff of agreed sanctions put in place.
The context, intention and impact of each incident should determine the response and actions to be taken. This allows a degree of flexibility in the application of sanctions. For example, a series of minor incidents by one individual is likely to be treated differently than a one-off occurrence; similarly unintentional and intentional access to inappropriate websites will instigate different levels of intervention and sanctions.
All online safety incidents should be recorded and monitored, and any potential patterns in behaviours identified, to enable such issues to be addressed proactively and for protectionbe afforded.

All incidents
The following procedure should be followed for all incidents:
 The incident should be reported to the Designated Safeguarding Lead. A written incident record should be made, and the situation monitored.
 The context, intention and impact of such misuse must also be considered. Where deemed necessary the incident may be escalated to a 'serious' level.
 If the incident relates to the inadvertent access to an inappropriate website, it should be added to the banned or restricted list and filters should be applied where relevant.
 In respect of misuse by children and young people, parents and carers must be informed of the alleged incident and should be advised of any actions to be taken as a result.

 Sanctions should be applied in accordance with the Acceptable Use Policy.

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 unsuitable in a childcare environment and should be acted upon.

Reporting

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

Serious incidents

 All serious incidents must be dealt with promptly and reported to the Designated Safeguarding Lead and the registered person immediately.
 The context, intention and impact of the alleged misuse must be considered.
 Appropriate actions should be agreed between the Designated Safeguarding Lead and theregistered person. All details should be accurately and legibly recorded. The reason why any decision is made should also be noted.
 If at any stage a child or young person is or has been subject to abuse in any form, the Safeguarding Policy should be implemented with immediate effect. A referral should be made through SPOA (Single Point of Advice) or through Children's Social Care and the Police, where applicable.
 If the incident relates 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 Child Protection and 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.
 No internal investigation or interviews should be carried out in respect of any allegations, unless explicitly requested otherwise by an investigating agency.
 If allegations of abuse are 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 taken which could compromise any such investigations.
 Where applicable, any hardware implicated in any potential investigations of misuse should be secured, so that evidence can be preserved. This may include mobile phones, laptops, computers and portable media technology.
 Internal disciplinary procedures should not be undertaken until investigations by the relevant agencies 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 appropriate, an online safety review should be undertaken and policies and procedures amended and updated as necessary. A consultation on any proposed revisions should be held with all ICT users as appropriate. Revised policies and procedures should be circulated as applicable.

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

 The following incidents must always be reported to the police, SPOA, 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.

 By not reporting such incidents, an offence may be committed.

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

 If potentially illegal material is discovered, as far as is reasonably practical, the equipment or materials found should not be touched. Computers or other devices should not be switched off unless 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 remains on).

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

A report should also be made to the Internet Watch Foundation if potentially illegal materials, including images of child abuse have been accessed online, giving details of the website address. If it is unclear whether the content is illegal or not, the concern should be reported as a matter of caution.

Media Attention

If a serious incident occurs, it may attract intense media interest and speculation. On such occasions, every possible attempt should be made to ensure that children and young people, parents and carers are protected and supported appropriately.
An agreed media strategy should be implemented, and statements only released by authorised personnel, in accordance with information sharing procedures. In all instances, the prime concern would be the safeguarding and welfare of the children, young people and their families.

Registered Charity No 1035670

Online Safety Incident Report Template

To be completed as thoroughly as possible by practitioner or manager identifying incident.

Date(s) / time(s) of incident:

Duration of incident: (e.g. one off, a week, 6 months etc.)

Description of the online safety incident: include detail of specific services or websites used (e.g. chat room, instant messenger); email addresses; usernames etc.

Why do you have concerns about this incident?

Has the information been recorded and secured? ☐ Yes, ☐ No

Has any computer or hardware been secured? ☐ Yes, ☐ No

If yes, who, where, when and what?Who was involved and how do you know this? Is there any evidence to suggest that false names / details have been given? Give full details of real names and email addresses etc. where known.

What actions were taken, by whom and why? Give detail of agencies informed and contact person within those agencies.

Name of person completing this form:

Name of setting:

Signature:
Date

Registered Charity No 1035670

Online Safety Incident Log

Date/ Time	Incident	Action taken – what?	Action taken – by whom	reported by	Signature

Guidance for Reviewing Internet Sites and Recording Log

This is the Guidance for Reviewing Internet Sites (for suspected harassment and distress). This guidance is intended for use when agencies need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that web site(s) concerned may contain child abuse images. If this is the case you must report the incident immediately to the police, SPOA, Children's Social Care, Local Authority Designated Officer and Ofsted.

Please follow all steps in this procedure:

 Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
 Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
 It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
 Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).

 Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  Internal response or discipline procedures.
  Involvement by Local Authority or national / local organisation (as relevant).
  Police involvement and / or action.

 If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child

- Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Record of reviewing internet sites (for suspected harassment / distress)

Setting:

Date:

Reason for investigation:

Details of first reviewing person;

Date:

Reason for investigation:

Details of second reviewing person;

Date:

Reason for investigation:

Name and location of computer used for review

Website(s) address	Reason for concern

Conclusion and action proposed or taken

Adoption of Policy

This policy was adopted at a meeting of the committee of Beckley Pre-School

Date: ……..

Signed on behalf of the Pre-School ……..

Print name of signatory: ……

Agreement to adhere to policy by staff

I confirm that I have read and understood this policy:

Name of staff member:
Signature: ……
Date: ……..

Name of staff member:
Signature: ……
Date: ……..

Name of staff member:
Signature: ……
Date: ……..

Name of staff member:
Signature: ……
Date: ……..

Name of staff member:
Signature: ……
Date: ……..

Name of staff member:
Signature: ……
Date: ……..

45.