NORTH STAR NURSERY AND HOLIDAY CLUB
TECHNOLOGY POLICY

1. Introduction

1.1 This policy is intended for the safety of children in our care and to protect the staff and students engaged with the children from unfounded allegations. Any breaches will be taken extremely seriously and could result in disciplinary action for misconduct. Misuse of social media could also lead to legal or criminal prosecution. This policy sets out expectations that North Star Nursery has of its staff, students and volunteers when using the internet and social media both outside and inside of working hours. The purpose of this policy is to identify proper usage and behaviour for the internet and social media applications used on a personal and professional basis with the overall aim of protecting the rights and privacy of staff and children in our care and the integrity and reputation of North Star nursery and Holiday Club.

1.2 All staff and students will be made aware of online safety procedures as part of their induction process and will be required to sign the Acceptable Use Policy (Appendix 5). North Star Nursery and Holiday Club will use training and guidance from the Swindon Safeguarding Partnership and Child Exploitation and On-Line Protection (CEOP) for staff training and when developing policies and procedures.

1.3 Staff, students and volunteers should be aware of the legislative framework under which this Technology Policy has been produced. This is set out at Appendix 1.

2. Telephone Use

2.1 North Star Nursery and Holiday Club provides its employees with access to the telephone for work-related purposes. We also provide access to mobile phones without cameras or internet access for emergency evacuations and off-site activities.

2.2 All staff and students can provide the main nursery (office) number for emergency contact situations e.g. to family members, schools or childcare providers.

2.3 All personal mobile phones must be placed in employees' lockers or in the office and access will only be allowed at break times, away from the children. North Star Nursery and Holiday Club does not accept responsibility for any valuables brought on to nursery premises.

2.4 If a staff member has a smart watch which can make calls and texts these must be disconnected from their phones whilst working so calls and texts cannot be answered.

2.5 Should a staff member in exceptional circumstances need their mobile phone to be available for a call, it will be agreed by the senior staff of the day and left in the office, where the individual can take the call should the need arise.

2.6 Any staff member found with their mobile phone about their person whilst engaged in childcare during working hours both on-site and off-site can be expected to be challenged by any parent or colleague and this may lead to disciplinary action.

2.7 If there is an urgent personal call that you need to make, then with the permission of the senior staff member present, you are able to use the office telephone or use your personal mobile, away from children, provided that this does not interfere with your work, nor take up an unreasonable amount of time.

3. Online Safety (e-Safety)

3.1 North Star Nursery and Holiday Club does not provide employees working with children access to the internet. Access to the internet is restricted to the office for use by the senior nursery team and office administrator for work-related purposes only, for example, for email correspondence with clients, internet banking, childcare voucher account management and weekly sun-strength checks. There may be occasions when staff, students or volunteers require to use the office computers for work-related purposes and this will be with prior agreement from a senior member of staff only.

3.2 There is no wi-fi within the nursery building and the children do not have access to online games. All games on the nursery iPads are app-based and do not require connection to the internet.

3.3 All personal internet enabled devices, including personal mobile phones, must be placed in employees' lockers or the office and access will only be allowed at break times, away from the children. North Star Nursery and Holiday Club does not accept responsibility for any valuables brought on to nursery premises.

3.4 Any staff member found with an internet enabled device about their person whilst engaged in childcare during working hours both on-site and off-site can be expected to be challenged by any parent or colleague and this may lead to disciplinary action.

3.5 North Star Nursery and Holiday Club are members of the 360° Early Years online safety programme which provides guidance on e-safety for organisations working with children with a view to policy and practices being regularly reviewed.

3.6 North Star Nursery and Holiday Club has relevant online safety/safeguarding policies and guidance. Staff, students, volunteers and all users must be aware of these guidelines which are included in this policy document. Staff, students, volunteers and users are also governed by relevant legislation, which is referred to in this policy and by the guidance provided by the Swindon Safeguarding Partnership (with regard to how incidents should be reported – see also ***Safeguarding and Child Protection Policy.***)

3.7 North Star Nursery and Holiday Club has an appointed an online safety designated lead, Julie Jones. Should any member of staff, parents or visitors have any concerns about online safety, they should approach the designated lead.

3.8 The Nursery Manager has overall responsibility for ensuring the safety (including online safety) of all staff, volunteers and members of the group. In the event of a serious online safety allegation being made against a member of staff, student or volunteer, the Nursery Manager will follow the procedures set out in the flowchart for reporting online safety incidents appended to this document at Appendix 2. The Nursery Manager is responsible for ensuring that the online safety designated lead and other relevant staff, students and volunteers receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

3.9 The online safety designated lead, in accordance with their job description, will be trained in online safety issues and be aware of the potential for serious child protection issues. **The designated lead is responsible for:**

(i) ensuring that staff, students and volunteers have an up to date awareness of the group's current Technology Policy and other online safety policy and practices
(ii) ensuring that all staff, students and volunteers are aware of the procedures that need to be followed in the event of an online safety incident taking place.
(iii) taking day to day responsibility for online safety issues and have a leading role in establishing and reviewing the Technology Policy

(iv) offering advice and support for all users
(v) keeping up to date with developments in online safety
(vi) understanding and knowing where to obtain additional support and where to report issues
(vii) ensuring relevant provision of training and advice for staff, students and volunteers
(viii) receiving reports of online safety incidents and create a log of incidents to inform future online safety developments)
(ix) communicating with parents and carers about relevant online safety issues
(x) monitoring incident logs
(xi) reporting regularly to the Nursery Manager.

3.10 **Staff, students and volunteers are responsible for ensuring that:**

(i) they have an up to date awareness of the nursery's current Technology Policy and practices
(ii) they have read, understood and signed the Acceptable Use Policy (see Appendix 5) and the Technology Policy
(iii) they report any suspected misuse or problem to the designated lead, Nursery Manager or senior member of staff – particularly where it is believed that a child's welfare is at risk
(iv) digital communications with children and young people are on a professional level and where possible only carried out using the official systems of the nursery
(v) children and young people in their care are aware of online safety where relevant and depending on their age
(vi) they are aware of online safety issues particularly those related to the use of mobile phones, cameras, gaming consoles and hand held devices and that they monitor their use and implement the nursery policies with regard to these devices.
(vii) confidentiality and organisational reputation are protected and the safety of the children in our care is paramount.

3.11 Staff and volunteers should act as good role models in their use of online technologies. North Star Nursery believes that the activities referred to in the following section would be inappropriate in a context of working with young people. **The Technology Policy restricts certain internet usage <u>at work and at home</u> as follows**:

(i) Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images, the making, production or distribution of indecent images of children contrary to the Protection of Children Act 1978
- grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003.
- possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and Immigration Act 2008
- criminally racist material in UK - to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986
- pornography
- promotion of any kind of discrimination
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the nursery or brings the nursery into disrepute.
- infringement of copyright
- revealing or publicising confidential information (e.g. financial / personal information, computer / network access codes and passwords)
- creating or propagating computer viruses or other harmful files

3.12 The Technology Policy restricts certain internet usage <u>at work</u> as follows:

(i) Use of systems applications, websites or other mechanisms that bypass the filtering or other safeguards that are in place
(ii) Unfair usage (downloading / uploading large files that hinders others in their use of the internet)
(iii) Using the group systems to run a private business
(iv) On-line gaming
(v) On-line gambling
(vi) On-line shopping/commerce (except for work purposes)
(vii) File sharing (e.g. Bit Torrent, Limewire)
(viii) Use of personal social networking sites
(ix) Use of video broadcasting (e.g. You Tube)

3.13 Where appropriate for their age, children and young people:

(i) are expected to abide by the Acceptable Use Policy ("Our Golden Rules") (see Appendix 6) which are displayed in the Holiday Club and Discoverers Rooms
(ii) need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
(iii) should demonstrate positive online behaviour.

3.14 Parents and carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parents and carers will be expected to sign relevant permission forms on the taking and use of digital and video images.

3.15 North Star Nursery and Holiday Club makes no provision for children in our care to access the internet. However, we are aware that the internet is part of everyday life and that children may well have access to Information and Communication Technology (ICT) at home and in other settings. Knowledge and experience of ICT is considered 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. The nursery iPads do not have internet access.

3.16 North Star Nursery will provide children and young people in our care with online safety awareness where appropriate. Key online safety messages ("Our Golden Rules") will be promoted as part of any relevant planned programmes of activities for the children and online safety issues will be discussed / highlighted if the occasion arises in informal conversations. "Our Golden Rules" for the use of devices / internet will be displayed in the Discoverers Room and in Holiday Club.

<u>4</u>. <u>Nursery Social Media</u>

4.1 All communications on the Nursery's social media accounts should be made through official channels using the nursery name. Where personal social media accounts associate themselves with or impact on the nursery, it will be made clear that the member of staff is not communicating on behalf of the nursery.

4.2 The nursery manager is responsible for monitoring the content posted on nursery social media. Staff may only upload content that is approved by the nursery manager or senior management in advance and which follows these rules:

(i) Only one person per room (per term) is to post relevant photos of children's work and the learning environment. The use of social media by staff whilst at work will be monitored and must not be excessive or interfere with relevant duties.
(ii) All photos should be uploaded from nursery cameras to the office computers prior to posting on social media.
(iii) All posts must come from the official nursery social media account and not from employees' personal social media accounts.
(iv) All posts must be linked to children's Next Steps, the EYFS, our curriculum or the nursery calendar of events.
(v) Under no circumstances must any content posted on nursery social media include names, photos or video recordings of children or clients.
(vi) Where staff may appear in photos or video recordings, their permission should be sought in advance of their use on social media.
(vii) Any content posted on nursery social media must be specific to North Star Nursery and what is happening within the rooms and the children's time at nursery.
(viii) Any content posted on nursery social media should be professional and respectful at all times through choice of words within the text. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgements about staff or the nursery. The nursery social media account must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the nursery.
(ix) Under no circumstances should any content be posted that will bring the nursery into disrepute.
(x) If a journalist makes contact about posts made using social media staff must not make any comment but refer them to the Nursery Manager in the first instance.
(xi) Unacceptable conduct (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality or copyright) will be considered extremely seriously by North Star Nursery and will be dealt with via the nursery's disciplinary procedure and escalated where appropriate. Where conduct is considered illegal, North Star Nursery may report the matter to the police and other relevant external agencies.
(xii) Parents/carers are encouraged to comment or post appropriately about the nursery. In the event of any offensive or inappropriate comments being made, the nursery will ask the parent/carer to remove the post and invite them to discuss the issues in person and, if necessary, these will be dealt with via the nursery's Complaints Procedure.

5. Personal Use of the Internet

5.1 Employees are fully responsible for their own actions and the consequences of their actions when accessing the internet and social media sites at any time.

5.2 Content posted on the internet and social media sites has the same legal status as written documents.

5.3 North Star Nursery and Holiday Club must ensure that confidentiality and organisational reputation are protected, and the safety of the children in our care is paramount. It is therefore essential that staff ensure proper practice when using the internet including social networking sites. This will also protect parents and other staff in the nursery, as well as your personal reputation.

5.4 Communication between adults and between children / young people 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, webcams, websites and blogs.

5.5 When using digital communications, staff and volunteers should:

(i) only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of North Star Nursery.

(ii) not share any personal information with a child or young person e.g. do not give personal contact details to children and young people including e-mail, home or mobile telephone numbers.

(iii) 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.

(iv) be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.

(v) ensure that all communications are transparent and open to scrutiny.

(vi) be careful in their communications with children so as to avoid any possible misinterpretation.

(vii) 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).

(viii) not post information online that could bring the nursery into disrepute.

(ix) be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

5.6 E-mail, text or other web based communications between staff / volunteers and a child / young person should (wherever possible) take place using the nursery's official equipment / systems.

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

Social Networking Websites

5.8 Staff members are allowed to use social networking sites, provided that they do not breach the law or disclose any confidential information about North Star Nursery and its clients, children and staff, breach copyright, defame the company or its suppliers, customers or employees; bring the organisation into disrepute, or disclose personal data or information about any individual that could breach the Data Protection Act 2018.

5.9 Staff members should be aware that social media websites are a public forum, particularly if the employee is part of a 'network'. Employees should not assume that their entries on any website will remain private. The content of social media websites could potentially remain online forever and is open to being republished in other media.

5.10 Employees should not use their own personal social media accounts to interact with parents on North Star Nursery's official social media pages unless with the specific agreement of the Nursery Manager as to content. Any content posted on the nursery's official social media pages should be agreed with the Nursery Manager prior to posting.

5.11 Specifically, staff members choosing to use social networking sites must follow the following guidelines:

(i) Ensure that your online profiles are private so that only friends are able to see your information. This can help to prevent any accidental breaches of this policy. Do not accept invitations to be friends from people you do not already know.

(ii) Be aware of the potential for on-line identity fraud and be cautious when giving out personal information about yourself which may compromise either your personal safety and security or that of children in your care.

(iii) Employees working with children should not identify themselves as working for North Star Nursery Ltd. Staff must not use the nursery logo or branding on their personal social media accounts.

(iv) Do not conduct yourself in a way that is detrimental to North Star Nursery, or that may be perceived by others as detrimental.

(v) Do not mention any of the children from the nursery or holiday club or their families/carers on social networking sites (apart from your own children, if appropriate).

(vi) Take care not to allow your interaction with others on these websites to damage working relationships between employees and clients of North Star Nursery and Holiday Club. Do not write anything detrimental about other staff members on social networking sites, or that may be perceived as detrimental.

(vii) In order to maintain professional boundaries staff should not invite or accept personal invitations to be friends from parents or carers that use the nursery and/or holiday club unless they know them in a personal capacity.

(viii) Staff must not write indirect suggestive comments about the nursery or holiday club that could have a negative impact on the reputation of the business, e.g. "I've had a bad day at work".

(ix) Do not mention any of the companies that North Star Nursery and Holiday Club works with on their social networking site.

(x) Staff must not use their own social media accounts to post information on behalf of the nursery unless with the specific prior agreement of the Nursery Manager as to content. In cases where any personal account is used which associates itself with the nursery or impacts on the nursery, it must be made clear that the member of staff is not communicating on behalf of the nursery with an appropriate disclaimer.

(xi) Staff are not permitted to follow or engage with current or prior children attending the setting on any personal social media network account.

5.12 All staff members should be aware that a breach of these guidelines will lead to disciplinary action. Any staff member aware of a colleague in breach of these guidelines has a responsibility to report this behaviour in confidence to the Nursery Manager, and failure to do so could also result in disciplinary action.

Cyber-bullying

5.13 North Star Nursery and Holiday Club is committed to ensuring that all of its employees are treated with dignity and respect at work. Bullying and harassment of any kind will not be tolerated in the work place. North Star Nursery can provide clear guidance on h**ow bullying and harassment can be recognised.**

5.14 **Cyber-bullying methods could include** using text messages, mobile phone calls, instant messenger services, by circulating photos or video clips or by posting comments on web sites, blogs or in chat rooms. Personal blogs that refer to colleagues without their consent is also unacceptable. Employees who cyber-bully a colleague could also face criminal prosecution under various laws, including the Malicious Communications Act 1988.

5.15 Further and specific information regarding offensive online behaviour can be found in the Technology Policy.

6. Monitoring

6.1 North Star Nursery and Holiday Club reserves the right to audit and monitor all aspects of employer provided electronic resources and electronic storage systems without notice, including the contents of any employee communication in these systems. This includes: email, data, voicemail boxes and other storage media.

6.2 The Nursery Manager will ensure that there is a system in place to allow for the monitoring of online safety in the setting and that they receive regular monitoring reports from the online safety designated lead. Reporting and Monitoring Logs are attached to this document at Appendices 3 and 4 respectively.

6.3 Users must immediately report to the online safety designated lead in accordance with this policy, the receipt of any communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such communication.

6.4 Any communication between staff / volunteers and the children / young people or their parents / carers must be professional in tone and content. These communications should, where possible, only take place on official (monitored) systems.

6.5 Personal information should not be posted on the nursery website and, where possible, only official email addresses should be used to identify members of staff.

7. Data Protection

7.1 All electronic data is subject to the Data Protection Act 2018 and is subject to the rules and regulations outlined in North Star Nursery's data protection policies with regard to usage, storage and destruction. For further information, please see the nursery's data protection policies:

- Privacy Notice – Clients
- Privacy Notice – Staff
- Data Breach Management Procedure
- Data Subject Access Request Procedure

7.2 Any electronic data that is shared is done so via secure systems such as Egress or DocSafe or is password protected.

7.3 Where North Star Nursery utilises a third party to process information on their behalf (a data processor), appropriate data sharing agreements/contracts are in place to ensure the data processor is compliant with the General Data Protection Regulation 2018.

7.4 North Star Nursery has procedures in place for the storage and destruction of electronic data in line with the requirements of the Data Protection Act 2018.

8. Password Security

8.1 The designated lead for online safety is responsible for ensuring that the technology used by the nursery is as safe and secure as is reasonably possible and that:

- users can only access data to which they have permission.
- access to personal data is securely controlled in line with the nursery's data protection policies.

8.2 Passwords and replacement passwords for shared computers and devices within the nursery, will be chosen by the Nursery Manager or senior member of staff and will be made available to staff, students and volunteers on a need-to-know basis only. Passwords will be changed at regular intervals. Users must keep passwords secure.

9. Photographs and Images

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

(ii) the making, taking and distribution of inappropriate and indecent images.
(iii) 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).

9.2 This policy will apply to all individuals who have access to and/or are 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 exhaustive. This policy applies to the use of any photographic equipment. This includes mobile phones and portable gaming devices with inbuilt cameras as well as other forms of digital technology and resources for storing and printing images.

9.3 The Designated Safeguarding Lead 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 Technology Policy and Acceptable Use Policy with regard to photographs and images.

9.4 This policy complies with the requirements of the Data Protection Act 2018, Freedom of Information Act 2000, Human Rights Act 1998 and other relevant Acts regarding the taking and use of photographic images of children. Further information regarding this legislation can be found at Appendix 1. All images will be used in a manner that meets the requirements of the Data Protection Act 2018.

9.5 The nursery has in place digital cameras for the purpose of taking images of children. Photographs and images can be printed directly from the camera and then deleted from the memory card without having to be saved to computer. This is to reduce the opportunity for photographs to be circulated electronically without parental permission. A small number of images can be retained by the Nursery Manager for a short time (no longer than 6 months) for the purposes of publicity in line with parental permissions.

9.6 As modern technology improves, most mobile phones and some games consoles are able to take images. Personal devices that can capture images will not be permitted in the play rooms by children, such as those attending Holiday Club, or by employees. Children may be allowed access to the nursery digital cameras or iPads as part of an activity; in which case the images should be printed directly from the device and then deleted unless they are going to be used for publicity in line with parental permissions.

9.7 The transferring of images via unprotected USB sticks, unfiltered web mail or via unprotected mobile media is not permitted. If remote access is given to servers or systems where images are to be stored, access will only be given as authorised by the Designated Safeguarding Lead.

Parental Consent

9.8 All staff and students should familiarise themselves with the parental consent forms for the photographing of their children for record keeping, display, publicity and website. Images of children who no longer attend the early years setting will not be used, unless specific consent has been obtained to cover this extended period.

9.9 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 will be accepted. Parents or carers 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. Such consent will detail how the images are to be used and for what period of time such permissions will cover.

Procedures with Regard to Capturing Images

9.10 Sensitivity must be shown to any child or young person who appears uncomfortable; and the potential for misinterpretation must be recognised. Images should therefore not be taken of any child or young person against their wishes.

9.11 The taking or making of images of a child or young person 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.

9.12 Photographs should not be taken of any child or young person 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 or young person 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 reporting procedures within the Safeguarding and Child Protection Policy should be implemented with immediate effect.

9.13 Images which may cause distress, upset or embarrassment must not be used.

9.14 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 at which shots are taken.

9.15 The taking or making of images in sensitive areas of the Nursery/Holiday Club, for example, toilet cubicles and changing areas is not permitted.

9.16 Where parents take photographs of their child at a group event, they should be aware of expectations of how that image may be used. Images and video should be for their own or family's personal use only and parents/carers should:

(i) think about privacy and who has the right to see their images, not only of their own child but of others;

(ii) 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.

9.17 The Nursery Manager reserves 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. All staff must ensure that all images are available for scrutiny and be able to justify any images in their possession, should it be necessary to do so.

Press Photography

9.18 There may be occasions where the press are invited to a planned event to take photographs of the children and young people 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. Parental consent with regard to this will be sought before the press is given access to any children or young people. If a parent or carer chooses not to give permission for their child to be photographed in such circumstances, this right will be observed at all times.

Professional Photography

9.19 The Nursery Manager will ensure 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:

(i) 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.

(ii) 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.

(iii) Photographers should be expected to demonstrate that they have agreed to ensure compliance with the Data Protection Act 1998 and that images are only used for a specified purpose and will not be used in any other context and that 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.

(iv) Details of any checks regarding suitability, which may include evidence of Disclosure and Barring Service (DBS) checks, will be requested.

(v) Photographic identity will 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 will 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 is given.

Parents and Carers Recording Images

9.20 Parents and carers are not permitted to use their mobile phones or any other device that can record or capture images within the nursery building, including the rooms and corridors, except with the prior permission of the Nursery Manager, for example, at events or special occasions.

9.21 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 will not be allowed.

9.22 Parents and carers who are authorised to use photographic equipment are 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.

Displaying Images

9.23 Images of children may be displayed around the nursery building in order to create a welcoming and familiar environment for the children. Photographs of individual children may also be displayed alongside their name in order to support their learning, for example, they may identify their own coat pegs by their photograph whilst learning to recognise their written name.

9.24 Parents and carers are reminded that the use of mobile phones and other devices that can capture and record images are not permitted in the nursery building, including the corridors and rooms where children's photographs may be displayed.

Learning Journeys and the Use of Images

9.25 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'. (Ref; Progress Matters, National Strategies). 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).

9.26 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 will be stored securely when not in use. The aim is to avoid unauthorised access to potentially sensitive data.

9.27 Individual learning journeys, constructed by practitioners, are provided for the benefit of the individual child and their parents or carers. Parents and carers therefore have 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 parents and carers of all children and young people captured in any of the photographs.

9.28 Photographs used within an individual child's learning journey will be of that child only. Should any other children in the setting be present in the photograph, their image will be redacted prior to its

inclusion within the learning journey, unless specific consent has been provided by the parent/carer to allow inclusion of their child's image within another child's learning journey.

Students and Training Portfolios and the Use of Images

9.29 During training, students and staff 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. Consent will be sought from parents and carers to use images of their children in these portfolios.

9.30 The Nursery Manager 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.

Photos on the Nursery Website and Social Media Pages

9.31 North Star Nursery will not post images of children in our care on to the nursery website, or any other website or social media site, to avoid the risk of unauthorised circulation and exploitation of images. Where photographs are posted of displays or the nursery rooms, any features that may identify children in our care within displays or on walls will be redacted. North Star Nursery is not responsible for photographs or images posted by parents or by others on their social media pages.

9.32 Photographs of staff will be posted on the nursery website only with the explicit written consent of the employee. Videos and images of staff may be uploaded to nursery social media only with the explicit written consent of the individual.

Storage and Disposal of Images

9.33 The nursery uses digital cameras where photographs and images can be printed directly from the camera and then permanently deleted from the memory card without having to be saved to a computer hard drive. This is to reduce the opportunity for photographs to be circulated electronically without parental permission. A small number of images may be retained by the nursery manager, and stored securely, for a short time for the purposes of publicity in line with parental permissions.

9.34 Images will not be kept for longer than necessary. Room leaders should ensure that all photographs are permanently wiped from digital camera memory cards once the images are no longer of use.

9.35 All images will remain on site at all times with the exception of learning journeys which will be sent home with parents and carers periodically for their perusal and comments. At these times, parents will be required to sign out the learning journey into their care and it will be signed back in to the nursery upon its return by a member of staff.

9.36 Printed photographs will be disposed of when no longer required. They will be returned to the parent or carer, deleted and wiped or shredded as appropriate.

9.37 Copies will not be taken of any images without relevant authority and consent from the Nursery Manager and the parent or carer.

9.38 A record of all consent details will 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 Relating to Photographs and Images

9.39 All images will be handled as personal data and deemed to be of a sensitive and confidential nature. It is recognised that damage or distress could be caused if security is breached.

9.40 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 Nursery Manager are required to take action as appropriate. All such incidents should be recorded, reported and acted upon.

9.41 Security procedures are monitored and reviewed regularly.

9.42 All staff, students and volunteers are required to follow confidentiality and information sharing procedures, which must be agreed to at the time of induction.

9.43 The following aspects of security are to be managed accordingly:

(i) Physical security - effective measures are in place to ensure physical security and to protect against theft, including that of laptops, computers, cameras, and any personal data, including photographic images. The nursery office is kept locked at all times when not in use.

(ii) Digital security – stringent measures are implemented to ensure digital security. Awareness should be raised in respect of technological advancements which could put online systems at risks. Security will be updated as and when required.

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

10. Staff Implications

10.1 All staff and students should familiarise themselves with the parental permission forms for the photographing of their children for record keeping, display, publicity and website.

10.2 As modern technology improves, most mobile phones and some games consoles are able to take images. Personal devices that can capture images will not be permitted in the play rooms or corridors by children, such as those attending Holiday Club, or by employees. Children may be allowed access to the nursery digital cameras or iPads as part of an activity; in which case the images should be printed direct from the camera and then deleted unless they are going to be used for publicity in line with parental permissions.

10.3 All employees will be required to keep their mobile phones and any other devices that connect to the internet or that can capture or record images in their lockers and will have access to mobile phones without cameras for emergency evacuations and off-site activities. All nursery staff and students will be expected to provide next of kin and own childcare provision with the main nursery land line number.

10.4 Should a staff member in exceptional circumstances need their mobile phone to be available for a call, it will be agreed by the senior staff of the day and left in the office, where the individual can take the call should the need arise.

10.5 This policy is for the safety of children in our care and to protect the staff and students engaged with the children from unfounded allegations. Any breaches will be taken extremely seriously.

10.6 Any staff member found with their mobile phone about their person whilst engaged in childcare working hours both on-site and off-site can be expected to be challenged by any parent or colleague, which may result in disciplinary action for misconduct. In addition, the circulation of photographs of the children taken during childcare working hours without the permission of the Nursery Manager and in line with parental permissions may also result in disciplinary action for misconduct.

10.7 All staff have a duty to report any concerns relating to potential misuse. Clear whistle-blowing procedures are in place and are set out in the Safeguarding and Child Protection Policy.

10.8 North Star Nursery follows effective safer recruitment procedures to ensure the reliability and suitability of any individual who has access to personal data. Rigorous and regular checks are also undertaken to ensure the on-going suitability of all new and existing staff, students and volunteers. All relevant checks are completed before any new employee, volunteer or student is given access to children and/or their personal data.

10.9 All staff, students and volunteers are required to follow confidentiality and information sharing procedures, which must be agreed to at the time of induction.

10.10 Staff should familiarise themselves with the North Star Nursery Code of Conduct which sets out specific guidelines for keeping themselves and the children in our care safe when using technology.

11. CCTV

11.1 CCTV may be used for the following purposes around the outside of the nursery building and the Polaris House site:

(iii) To control access.
(iv) To monitor security.
(v) For site management, for example monitoring incorrect parking, manoeuvring vehicles and delivery arrivals.
(vi) To act as an effective deterrent to prevent crime and to discourage trespass.

11.2 All areas which are covered by CCTV around the site are well signposted, CCTV around the Polaris House site is subject to the Polaris House Site Security Policy July 2020 and which is appended to the North Star Nursery Security Policy.

11.3 The nursery utilises CCTV cameras at the nursery main entrance and in the garden during winter periods when it is dark outside for security reasons. Images may be recorded and held for a period of time as set out in our Data Protection Policies.

References

1. Early Years Alliance
2. Data Protection Act 2018
4. Early Years E-Safety Checklist
5. Guidance for Safer Working Practice for Adults who work with Children and Young People
6. 360 Early Years Tool Self-Review Tool
7. Polaris House Site Security Policy July 2020
8. SWGfl Social Media Policy Template January 2020

This policy links to:	Acceptable Use Policy for Staff "Our Golden Rules" (AUP for Children) Health and Safety Policy Health and Safety Staff Handbook Safeguarding and Child Protection Policy Code of Conduct Privacy Notice – Clients Privacy Notice – Staff Data Protection Breach Management Data Subject Access Request Procedures Risk Assessment Policy Confidentiality Policy Equality, Diversity and Inclusion Policy Positive Behaviour Management Policy Security Policy & Polaris House Site Security Policy Safer Recruitment and Induction of Staff, Training and Development Policy Student Partnership

Policy Review History	
April 2013	v.1
August 2015	v.2
October 2016	v.3
October 2017	v.4
August 2018	v.5
May 2021	v.6
July 2021	v.7
July 2022	v.8

This policy will be reviewed in July 2023 unless a review of events, legislation or guidance from health professionals or Ofsted indicates that a review should take place sooner.

Signed …… Dated ……

Print …… Nursery Manager

Signed …… Dated ……

Print …… Reviewing Committee Member

Appendix 1

Legislative Framework for this Policy

It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the event of an online issue or situation.

Computer Misuse Act 1990
This Act makes it an offence to:
• Erase or amend data or programs without authority;
• Obtain unauthorised access to a computer;
• "Eavesdrop" on a computer;
• Make unauthorised use of computer time or facilities;
• Maliciously corrupt or erase data or programs;
• Deny access to authorised users.

Data Protection Act 2018
The Data Protection Act 2018 brings data protection law in line with how people's data is being used. It gives organisations more clarity over the legal environment that dictates how they can behave and ensures data protection law is almost identical across the EU following the General Data Protection Regulation 2018.

GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:
• Establish the facts;
• Ascertain compliance with regulatory or self-regulatory practices or procedures;
• Demonstrate standards, which are or ought to be achieved by persons using the system;
• Investigate or detect unauthorised use of the communications system;
• Prevent or detect crime or in the interests of national security;
• Ensure the effective operation of the system.
• Monitoring but not recording is also permissible in order to:
• Ascertain whether the communication is business or personal;
• Protect or support help line staff.
• The nursery reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -
• Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
• Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening.

Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006, it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the context of work with young people, human rights to be aware of include:
• The right to a fair trial
• The right to respect for private and family life, home and correspondence
• Freedom of thought, conscience and religion
• Freedom of expression

• Freedom of assembly
• Prohibition of discrimination
• The right to education.

These rights are not absolute. The nursery is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

This Act empowers school headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

APPENDIX 3

ONLINE SAFETY REPORTING LOG

Report made by:						
DATE	**TIME**	**INCIDENT**	**ACTION TAKEN**		**INCIDENT REPORTED BY**	**SIGNATURE**
			What?	**By whom?**		

APPENDIX 4

ONLINE SAFETY MONITORING LOG

COMPUTER / DEVICE MONITORED	MONITORED BY	ISSUES IDENTIFIED	ACTION TAKEN		SIGNATURE
			What?	By whom?	

APPENDIX 5

NORTH STAR NURSERY AND HOLIDAY CLUB
ACCEPTABLE USE POLICY

This Acceptable Use Policy is designed to support the Technology Policy and must be read in conjunction with this document.

This policy is intended to ensure that staff, students and volunteers will act responsibly to stay safer while online, being a good role model for the children in our care and to ensure that effective systems are in place for the online safety of all users and the security of devices, systems, images, personal devices and data. This policy is also intended to ensure that staff, students and volunteers are aware of and can protect themselves from potential risk in their use of online technologies.

Acceptable Use Agreement

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

For my professional and personal safety, I understand that:

- I will ensure that my online activity inside and outside of work does not compromise my professional responsibilities, nor bring the nursery into disrepute. I will ensure that I do not post online derogatory remarks about my colleagues or my employer which could be seen by clients, colleagues or managers.

- My use of technology could be monitored.

- When communicating professionally I will use the technology provided by the nursery (e.g. email, Teachers2Parents, etc.). I understand that there may be risks attached to using my personal email address / mobile phone / social networking sites for such communications. I will only use nursery technology for company business and not for expressing my own views.

- These rules also apply when using North Star Nursery technology either at home or away from the premises.

- Personal use of the nursery's technology is only acceptable with permission from the Nursery Manager or senior member of staff.

- Any social media account that I hold must be made and kept private. I will not use the nursery's logo or branding on my personal social media accounts.

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 and in line with the nursery's data protection policies for clients and staff.

- I understand that any images I publish will be with the owner's permission and follow the nursery's code of practice.

- I will not use personal equipment to record any digital and video images, unless I have permission to do otherwise.

For the safety of the group, I understand that:

- I have read and understood the Technology Policy.

- 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 and young people in my care

- I will not deliberately bypass any systems designed to keep the nursery safe.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Privacy Notices for staff and clients. Where personal data is transferred, externally, it must be encrypted or password protected. Passwords will be sent to the recipient via separate email or telephone.

- I understand that the nursery data protection policies require 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 nursery's policies 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 not use or carry any personal device that can take and/or record images in the children's rooms at any time and will ensure that any such device that I bring on to nursery premises is kept locked in my locker during working hours.

- I will inform the appropriate person if I find any damage or faults with technology I am using at nursery.

- I will not attempt to install programmes of any type on to devices belonging to the nursery, without permission of the Nursery Manager or senior member of staff.

Signed ……

Print Name ……..

Date ……..

Appendix 6

OUR GOLDEN RULES

This is how we stay safe when we use technology:

I will ask an adult / a leader if I want to use technology.

I will only use activities that an adult / a leader has told or allowed me to use.

I will take care of the PlayStation, Wii, iPads and other equipment.

I will ask for help from an adult / a leader 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 technology.