

Online Safety & Security Policy

**For the Pen Green and Kingswood Integrated Centre
(comprising Pen Green Nursery School, Early Years Setting, Research & Training Base, Integrated Services and Corby Children Centres)**

Online Security Policy

Reviewed September 2025

Introduction

At Pen Green & Kingswood Integrated Centre, we are committed to keeping all children, families, and staff safe online. This policy sets out how we use technology responsibly, protect personal data, and ensure that our IT systems are secure. It also provides clear guidance for staff, parents, and visitors so that together we create a safe and supportive digital environment.

The Governors and the Centre Leadership Team appreciate that electronic communications are an essential element in 21st century life for education, business and social interaction. We wish to support the children in using ICT as part of their learning experience and believe that used correctly ICT will raise standards, support staff in their work, and will enhance the Integrated Centre's management information and business administration systems.

All early years' settings have a duty to ensure that children are protected from potential harm both within and beyond the learning environment. Every effort will be made to safeguard against all risks; however, it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children and staff continue to be protected.

The Integrated Centre, through its filtering and monitoring of website activity across the Centre, will ensure that any relevant activity taking place that may be within the scope of the PREVENT Duty will be followed up and logged with the appropriate body.

Aims

- To offer valuable guidance and resources to early years settings and practitioners to ensure that they can provide a safe and secure online environment for all children in their care.
- To raise awareness amongst staff and parents/carers of the potential risks associated with online technologies, whilst also highlighting the many educational and social benefits.
- To provide safeguards and rules for acceptable use to guide all users in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the early years setting.

Scope of Policy

This policy applies to all staff, children, parents/carers, students, professionals, visitors and contractors accessing the internet or using technological devices on the premises. This includes the use of personal devices by all of the above-mentioned groups, such as mobile phones or iPads/tablets which are brought into an early years

setting. This policy is also applicable where staff or individuals have been provided with setting issued devices for use off-site, such as a work laptop or mobile phone.

Practitioner responsibilities (including volunteers)

All staff have a shared responsibility to ensure that children are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all adults working with children are bound.

Please see North Northants Council (NNC) Acceptable Use Policy for Employees for further details regarding staff responsibilities and expectations for behaviour whilst accessing the internet, email, or related technologies within and beyond the early years setting.

For those staff using desktop NNC networked computers the responsibility of appropriate usage by staff is outlined in the above policy. Maintenance and security of the system is the responsibility of West Northants Council (WNC).

In the nurseries and early years settings staff use Apple iPads and laptops, of which all of these have access to the Centre's Wi-Fi system. The Integrated Centre's Marketing and Communication Officer and the Social Media Officer use IMacs fitted with facial recognition software. To support practitioner and administration functions there are several Windows based laptops and Notebooks.

Staff Training

All staff are required to complete annual training in:

- Data Protection (GDPR)
- Cyber Essentials / online safety awareness
- PREVENT

New staff must receive online safety and data protection training as part of induction.

The Centre Administration Team monitors completion of this training to ensure full staff compliance. Records are maintained and reported to the Head of Centre as part of the Centre's safeguarding and compliance responsibilities.

In addition, all staff share responsibility for modelling safe and respectful use of technology and for supporting children to develop age-appropriate online safety awareness as part of their everyday learning.

PREVENT Duty

In line with the Counter-Terrorism and Security Act 2015, the Integrated Centre recognises its duty to have due regard to the need to prevent people from being drawn into terrorism. All staff receive training to recognise indicators of radicalisation and extremist influence, including those that may occur online.

Any PREVENT-related concerns will be reported immediately to the Designated Safeguarding Lead, who will take appropriate action in line with safeguarding procedures. This may include referral to the Local Authority PREVENT team, Police, or other external safeguarding partners.

The Centre works in partnership with the Northamptonshire Safeguarding Children Partnership and other statutory agencies to ensure concerns are addressed promptly and proportionately.

Parents

In addition, parents can access the Centre's Wi-Fi system whilst they are in the building. As mentioned earlier any activity detected that may fall within the scope of the PREVENT duty will be duly reported to the appropriate body.

Site Administrator responsibilities

To ensure appropriate use of the Wi-Fi system this is overseen by the Site Administrator who has full access to the system and can make changes. In addition, the site administrator is responsible for:

- Instalment of Anti-virus software and supporting staff to ensure regular software updates are undertaken to maximise and maintain security on all setting machines and portable devices.
- Ensuring that users may only access the Integrated Centre's network through a rigorously enforced password protection process, in which passwords are regularly changed.
- Applying and updating the Integrated Centre's filtering policy on a regular basis.
- Reporting to the Head of Centre or DSL when restricted sites have been accessed.
- Any problems or faults relating to filtering are immediately logged and recorded on the Online Incident Log and action taken as appropriate.
- Monitoring the use of websites to ensure that any relevant activity related to the Prevent Duty is recorded and acted upon.
- Undertaking regular audits of staff IT equipment to ensure usage is within the Integrated Centre Online Safety Policy and NNC Acceptable Use policy.
- In conjunction with the Deputy and Assistant Head in the research base the provision and management of virtual software used in blended learning and service delivery.

Governor responsibilities

For overseeing the information technology systems, the Centre has a named Governor who is responsible for ensuring that:

- The Integrated Centre's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Keeps up to date with e-safety technical information to maintain the security of the network and safeguard children.

- An overview of the use of the Integrated Centre's network.
- Monitoring of the network and checking any deliberate or accidental misuse has been reported via the Site Administrator to the Head of Centre or Designated Safeguarding Lead.
- There are two named governors who hold responsibility for GDPR.
- Governors will review and challenge online safety practice annually, using the Head's report as evidence.

External contractor responsibilities

In general, external contractors will only have access to Centre network attached systems and software to complete contracted tasks.

External contractors shall:

- Be retained under commercial contract for a specific purpose as directed by the Head or an authorised member of staff as designated by the Head.
- Only install hardware and software as required to fulfil contracted services.
- Provide secure administrator access to the Site Administrator for all network attached systems and software provided to the Centre by the contractor once configured and operational
- Provide necessary training or instruction to the Site Administrator as directed by the Head of Centre or the Chair of Governors regarding the provision of the above point.
- Ensure that the safety and security of the Centre and its IT systems are not compromised as a consequence of any contracted activities.
- Observe and comply with the Online Safety & Security Policy regarding their activities when using Centre network resources and equipment.

Broadband and Age-Appropriate Filtering

Broadband provision is essential to the running of an early years setting, not only allowing for communication with parents and carers but also providing access to a wealth of resources and support. The Integrated Centre staff use internet enabled devices, including iPads to enhance the learning experience of children and as online tools for staff to track and share achievement. For this reason, great care must be taken to ensure that safe and secure internet access, appropriate for both adults and children, is made available regardless of the size of the Integrated Centre. It is ultimately the responsibility of the Centre Leadership Team to ensure that the internet provision at the Integrated Centre' is as safe and secure as is reasonably possible.

The Marketing and Communication Officer is the named administrator responsible for reviewing filtering and monitoring systems. Reviews are undertaken termly alongside the DSL to ensure that both a safeguarding and IT perspective are considered.

Age and user appropriate content filtering is in place across the Integrated Centre, ensuring that staff and children receive different levels of filtered internet access in

line with user requirements (e.g. YouTube at staff level but blocked to children and centre users)

Any changes to filtering levels are documented on the Filter Change Request Log (see *attached template document*) and include the reason for the requested change, the date and name of staff member concerned.

Parental controls are established on all internet enabled devices that children have access to, blocking or preventing access to any harmful, illegal, or inappropriate content.

Filtering levels are managed and monitored on site via an OpenDNS administration tool/control panel, provided by our broadband supplier, which allows an authorised staff member (Marketing & Communication Officer) to monitor access to sites and manage user internet access.

Reviews are undertaken to record what network activity is happening and look for patterns in blocked sites.

Monitoring, Reporting and Review

The Marketing and Communication Officer and the Designated Safeguarding Lead (DSL) will meet termly to review filtering and monitoring activity. These meetings will include:

- Reviewing blocked/flagged sites and activity logs.
- Assessing whether filtering and monitoring remain appropriate to the Centre's safeguarding risk profile.
- Considering any recent safeguarding reports or incidents linked to online activity.
- Recommending changes to filtering or monitoring procedures.

A record of these termly reviews will be kept.

In addition, the Head of Centre and Marketing and Communication Officer will prepare an **annual report to Governors** summarising:

- The effectiveness of filtering and monitoring.
- Key safeguarding trends from incident logs.
- Any updates to policy or practice.

This ensures that governors fulfil their statutory duties under *Keeping Children Safe in Education (2024)* by receiving regular oversight of online safety arrangements.

Email Use

Staff

- The Integrated Centre and NNC provide appropriate staff with access to a professional email account to use for all work-related business, including communication with parents and carers. This includes NNC Outlook; and

6 Linked documents: KCSIE 2025; www.ceop.police.uk/Safety-Centre/; NNC Acceptable Use policy; Working Together to Safeguard Children

Office 365 email accounts. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.

- Staff must not engage in any personal communications through social medium (i.e. via Hotmail or yahoo accounts etc.) with parents of children for whom staff have a professional responsibility (not withstanding those who were already friends) and with children who they have a professional responsibility for. This prohibits contact with former pupils outside of authorised setting email channels also.
- All emails should be professional in tone and checked carefully before sending, just as an official letter would be. This includes those that are sent internally as well as externally.

NNC information governance guidance states:

- Do not email any council (centre) related information or documents to personal email accounts.
- Check the addressee before pressing 'send' especially when using autofill.
- The retention timeframe for emails is 12 months, staff to ensure a regular cleansing exercise on mailboxes is carried out.
- To remove sensitive or confidential attachments at point of receipt and place in separate folders.
- Any emails needing to be retained should not be held in Outlook they should be saved to the relevant network folder.
- At the point of which staff leave the organisation access to all email accounts and virtual platforms provided by the Integrated Centre is removed.

Students

- The Integrated Centre provides students with access to a professional email account to use for all study related activities, including communication with tutors and consultants.
- 6 months following the point at which students complete their period of academic study access to their organisational email account is removed.

Use of Social Networking Sites (advertising or parental contact)

Social networking sites (e.g. Facebook and Twitter) can be a useful advertising tool for early years settings and can often be an effective way of engaging with young or hard to reach parents. Due to the public nature of social networking and the inability to keep content truly private, great care must be taken in the management

and use of such sites. Best practice guidance states that:

- Identifiable images of children must not be used on social networking sites without specific consent first being sought from those who have legal responsibility for the children. Staff must always adhere to our use of photograph policy.
- To maintain professional distance and to avoid unwanted contact, staff should not link their personal social networking accounts to the Integrated Centre' page unless it is to promote marketing materials.
- Ensure that privacy settings are set to maximum and checked regularly, unless we are using the sites for marketing purposes then specific consent will be sought for the use of any image and materials. We will make it clear on the consent paperwork that the images will be on a link that is open for public use.
- For safeguarding purposes, photographs or videos of looked after children must not be shared on social networking sites.

Mobile/Smart Phones/Smart & Sport Watches

Staff:

- Personal mobile phones and access to smart and sport watches that are capable of receiving/sending data and/or communications are permitted on the Integrated Centre' grounds, but are to **be used during break times only, within designated areas away from children.**
- The wearing of smart and sport watches by children attending any of the settings in the Integrated Centre is not allowed given the potential for unauthorised/unintentional taking of photographs and/or video recording within the setting.
- Staff **should not** have phones, or smart/sport watches on their person during work hours, if you see a colleague using their mobile phone or a smart/sport watch within work time there is the expectation that you will challenge this inappropriate use and request the phone be put away. Should this practice continue despite a colleague's challenge it needs to be reported to a member of CLT.
- Personal mobile phones or smart/sport watches must **never** be used to contact children or their families, nor should they be used to take videos or photographs of children. Integrated Centre issued devices only should be used for this purpose and, if containing sensitive information or photographs of children, should not leave the premises unless encrypted and this must be acknowledged in the policy.
- The only exception to this policy is in the event of where normal or usual communication channels are not available. This type of contact can only be authorised by the Head/Deputy Head of Centre.
- For staff who are allocated a work mobile phone, access to the local authority system requires the use of two factor authentication. This process requires access to personal mobile phones by staff to receive the required code to use on their work devices. This is the **only permissible work-related use of staff personal phones.**

Parents / visitors / Centre Users

In line with the most up to date guidance from the Department of Education (2024) regarding mobile usage in school settings, mobile phones brought into the Integrated Centre are **prohibited** from being used across the Centre by parents/carers, visitors, or centre users. There is one designated area (the Community Room). This is where parents can make/receive urgent or emergency calls relating to their child(ren) or family's well-being or physical health. Staff will be expected to consistently follow the policy and ensure parents/Visitors/Centre Users adhere to the policy while in the Centre.

Photographs and Video

Digital photographs and videos are an important part of the learning experience in the Integrated Centre and, as such, staff have a responsibility to ensure that they not only educate children about the safe and appropriate use of digital imagery but also model good practice themselves. To this end, there are strict policies and procedures for staff and children about the use of digital imagery and videos.

- Written consent must be obtained from parents or carers before photographs or videos of young people will be taken or used within the Integrated Centre including displays, learning journeys, setting website and other marketing materials.
- Staff will ensure that children are at ease and comfortable with images and videos being taken.
- Staff must not use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of children.
- Integrated Centre issued devices only should be used for this purpose and, if containing sensitive information or photographs of children, should not leave the premises unless encrypted and this must be acknowledged in the policy. In the case of an outing, all data must be transferred/deleted from Integrated Centre' camera/device before leaving the premises.
- Consent is collected for all staff, volunteers, students, and governors in order to ensure that images are only used where there is specific consent.

Laptops/iPads/Tablets

Staff Use:

- A log of all ICT equipment issued to staff, including serial numbers, is maintained by the Integrated Centre Asset Management System. All staff accessing setting equipment are required to complete a Safe User Agreement (Appendix 1) at the point of issue of equipment.
- Personal use of setting laptops or computing facilities, whilst on site, is left to the discretion of the Centre Leadership Team and may be permissible if kept to a minimum and only during authorised breaks.
- Where staff have been issued with a device (e.g. setting laptop) for work purposes, personal use whilst off site is permitted, however a separate account

9 Linked documents: KCSIE 2025; www.ceop.police.uk/Safety-Centre; NNC Acceptable Use policy; Working Together to Safeguard Children

must be set up on the device so there is no way the information stored about children and families can be mixed up with anything stored on the device for personal use. Integrated Centre' laptop/devices should be used by the authorised person only.

- Staff are aware that all activities carried out on setting devices and systems, both within and outside of the work environment, will be monitored in accordance with this policy.
- Staff will ensure that setting laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades, or routine monitoring/servicing. It is at this time a scan will take place to see what the device has been used for. Any inappropriate use will result in disciplinary processes being followed.
- Setting issued devices only should be used for this purpose and, if containing sensitive information or photographs of children, should not leave the premises unless encrypted and this must be acknowledged in the policy.
- **Please note: The Head of Centre are ultimately responsible for the security of any data or images held of children within the Integrated Centre.**
- Support is provided to staff in the use of IT equipment in the form of both 1:1 training and specifically devised User Guides. For further information please contact the Integrated Centre Marketing & Communications Officer.

Children's Use:

- Laptop, iPad or tablet use must be supervised by an adult at all times and any games or apps used must be from a pre-approved selection checked and agreed by the Assistant Heads.
- Online searching and installing/downloading of new programmes and applications is restricted to authorised staff members only. Children should not be able to search or install anything on a setting device.

Children's Online Safety Education

In line with *Keeping Children Safe in Education (2024)*, the Integrated Centre recognises the importance of supporting children to develop the skills, knowledge, and confidence to use technology safely and responsibly.

Children are introduced to online safety concepts in age-appropriate ways through play, guided exploration, and adult-led discussions. This includes:

- Learning to ask for help and tell a trusted adult if they see or experience something that worries them.
- Understanding simple rules for using devices safely (e.g. staying on apps or websites chosen by adults).

- Developing respect for others when using technology, including safe and kind communication.
- Recognising that photographs, videos, and personal information should be shared only with adult guidance and consent.

These principles are embedded across the curriculum and daily practice so that children begin to build early digital citizenship skills. Staff model safe and respectful use of technology at all times to reinforce these messages.

Applications (Apps) for recording pupil progress

Applications are available to allow staff to track and share a child's learning journey online with parents and carers, usually in the form of photographs and text. Such tools have considerable benefits, including improved levels of engagement with parents and a reduction in paperwork, but careful consideration must be given to safeguarding and data security principles before using such tools.

- **Personal staff mobile phones or devices (e.g. smart/sport watches, iPad or iPhone) should not be used for any apps which record and store children's personal details, attainment or photographs. Only setting issued devices may be used for such activities, ensuring that any devices used are appropriately encrypted if taken off site. This is to prevent a data security breach in the event of loss or theft.**
- Before purchasing or accessing any apps for staff or children's use, senior staff must have a clear understanding of where and how children's data will be stored, including who has access to it and any safeguarding implications. Please note: The Head of Centre are ultimately responsible for the security of any data or images held of children within Pen Green.

Applications and Programmes for use of online Teaching

- Applications such as Microsoft Teams and Zoom are used for virtual delivery of Higher and Further Education courses delivered by the Research, Training and Development Base. These applications are only to be accessed and used with Centre issued accounts and devices.

Users of these platforms are expected, at all times to behave in a professional manner, and to comply with the Centre Policies regarding GDPR and Data Protection.

Data Storage and Security

The General Data Protection Regulations 2018 (the Act) applies to anyone who handles or has access to information concerning individuals. The new regulations build upon the principles of the previous Data Protection Act (1998). Everyone in our setting has a legal duty to protect the privacy of information relating to individuals.

The Regulations set standards, which must be satisfied when processing personal data (defined as information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

Individuals' rights include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object; and
- The right not to be subject to automated decision-making including profiling.

The quantity and variety of data held on pupils, students, families and on staff is always expanding. Whilst this data can be very useful in improving services, data could be mishandled, stolen or misused. The Governors are aware that the security of personal data is always paramount and ensure that all portable media, such as external hard drives and memory sticks, can only be used if they are password protected.

The Regulations promotes openness in the use of personal information ensuring that every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Centre is registered with the Commission, and its Registration number is **ZA130051**.

Sensitive data, photographs and videos of children are not stored on setting devices which leave the premises (e.g. laptops, mobile phones, iPads, USB Memory Sticks etc.) unless cloud based or appropriate encryption software is in place.

In relation to all data that leaves the Integrated Centre the relevant consents will need to be in place and a log kept of all hardware/software taken to an alternative site.

This applies to Research training offsite, material taken abroad (EECERA) and any other delivery other than at the Integrated Centre site.

Assessing Risk

The Centre will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the Centre network.

The Centre cannot accept liability for any material accessed, or any consequences of Internet access. Methods to identify, assess and minimise risks will be reviewed regularly.

The Head of Centre and Governors will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Useful Links

- Northamptonshire Safeguarding Children's Partnership (NSCP).
Online Procedures: www.nscbnorthamptonshire.org.uk
- <https://www.nctrust.co.uk/help-and-protection-for-children/protecting-children-information-for-professionals/Pages/bullying-and-online-safety.aspx>
- Data Protection and Freedom of Information advice: www.ico.org.uk

Appendix 1 Safe User Agreement

Username:

This agreement applies to any device (e.g. laptop, mobile phone, iPad, memory stick) which has been issued by the Centre.

This agreement must be signed before any device provided by the Centre is removed from the premises.

Passwords and encryption

- All devices in possession of the user will be password protected
- Any device will only be used by the authorised user
- All accounts will have been set up (or re-set for older equipment) by the Site Administrator using organisational based information. Staff are **not** allowed to change either the set-up, passwords or PIN numbers allocated to that device.
- Tapestry – accounts not to be transferred to internal/external/other settings when child leaves Pen Green/Kingswood settings.
- Organisational Apple products are not to be connected to any other iCloud account
- The user will never share passwords. Access to Outlook accounts can be requested through NNC by supervisors in the case of extended periods of leave by staff to ensure business continuity.
- Any device that can be used to access data will be locked by the user if left (even for very short periods) and set to auto lock if not used for five minutes.
- NNC emails can now be accessed on a range of devices and staff should ensure that they do not leave their NNC accounts constantly signed in. Staff are required to log out on each occasion of accessing their email account on mobile devices.
- Updates – staff need to regularly complete Updates on machines as and when they arise and not leave them for long periods of time.
- Should the device be used for personal reasons, a separate user account will be set up so that information held on children and families cannot be mixed up with personal information.
- Staff are responsible for existing equipment and access to that equipment, where access may be lost/not recorded (PIN number or password) centrally by

the worker and the item becomes defunct staff may be required to replace that item.

- All devices, including memory sticks or other removable media, will be encrypted using approved encryption software.

Transportation and storage

- All storage media will be transported and stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation
- All workers are required to ensure that they have appropriate home insurance arrangements in place that covers any electronic equipment they are responsible for in the event of damage or theft.

Handling data

- Private equipment (i.e. Owned by the user) will not be used for the storage of any personal data related to users of the Centre.
- Tapestry – accounts not to be transferred to internal/external/other settings when child moves setting.
- Data will be securely deleted from any device, (i.e. deleted permanently and/or securely overwritten) once it has been transferred or its use is complete.

Monitoring

- The user will make any device available on request for routine monitoring in accordance with the Centre's Online Safety Policy

Device: Serial No:

Phone Number (mobile):

Asset Number:

Signed:..... **Date:**.....

In signing this document, you are agreeing to follow the processes outlined above. Any inappropriate use or failure to follow the above processes may result in the equipment being confiscated and/or relevant HR processes being invoked.

Additional Notes for Consent Process for Photography, Filming and Social Media

There are four processes across the Integrated Centre in relation to consent for a variety of media as outlined above.

Children in Nest, Couthie, Kingswood, Nook & Nurseries (Form A)

During the Home Visit parent/carers are asked to complete the consent paperwork for their child(ren) whilst in any of the education and care settings. Once received this information is recorded on the Consent spreadsheet held by the Marketing Officer. This spreadsheet also holds additional information in relation to children not to be photographed or filmed, including Children in Care. The use of images are as defined within the Online Safety Policy.

During the early stages of a new intake of children the Marketing Officer and the Social Media Officer will visit the different settings in order to build relationships with children and their families prior to any images being taken. This exercise is repeated on a bi-annual basis. Children's own verbal consent to having their photograph taken is also sought when actual photography is taking place.

In addition to the Consent spreadsheet, the use of digital recognition is also used on the iMac. This enables all images of a single child to be grouped together and also to demonstrate that consent is held for the images. The consent is linked to the Integrated Centre Online Safety Policy which states that images of children will be held for a maximum period of 3 years.

The digital recognition enables the Marketing Officer to monitor and review the timelines in relation to the images held. The Marketing Officer will undertake regular annual cycles of removing images in line with the Online Safety Policy. The only exception to this will be where specific consent has been given by parents/carers for use within the Integrated Centre published material and the historic archive. Published material once in the public domain will no longer be subject to the Integrated Centre Online Safety Policy.

Groupwork & Children's Centre (Form B)

This process is slightly different to the above given that the focus group is much wider and more transient and covers a much greater set of physical locations including the activities of Corby Children Centre, which is the reason for all four logos on the document. Consent forms are distributed by group leaders/individual workers to gain consent from families.

This consent needs to be logged with the Marketing Officer prior to any photographs, filming or social media use being undertaken. Verbal consent will also be sought from parents and children at the time of photographs being taken. Digital recognition then serves to group images by event and highlight retention timescales.

Staff, Student, Volunteer & Governor Consent (Form C & C.1)

Consent is sought from all individuals within these groups to have their images used for a variety of reasons to support professional development and promote the services of the Integrated Centre.

Form A Consent for Film/Photography within Nursery, Nook, 0-3yrs spaces

Within the setting we regularly use digital photography and video to document children's learning. We also use images to promote the work of the setting which includes information for parents and carers, staff development and professional training and promotion of the Centre services through social media.

Child's Name:

Date of birth:

Tapestry is an online document of your child's learning whilst in nursery and our 0-3 settings, which parents/carers can access through a secure online portal. We also have a paper version of this documentation, and this is kept in your child's 'Celebration of my Achievements' file. For more information about *Tapestry* please speak to your Family Worker. (For Nook children this does not apply as *Tapestry* not used).

We take the utmost care to ensure that your child's wishes are respected and that only positive images of your child are displayed. We understand that children spend time learning collaboratively and enjoy many friendships and, therefore, there may be times when an image of your child features in a photograph in another child's file.

I agree to my child being photographed and filmed for children's files:

Paper version:

Yes/No*

Online Version:

Yes/No*

I agree to images of my child featuring in other children's paper files:

Yes/No*

I agree to images of my child featuring in other children's online files:

Yes/No*

I agree to my child being photographed and filmed for Integrated Centre displays and/or promotional paper material relating to the Integrated Centre.

Yes/No*

Staff Development - we also use video and digital images for staff development within the centre. These images will not be made available to a wider audience without your full consent.

I agree to my child being photographed and filmed for use in staff development opportunities:

Yes/No*

Website – the Integrated Centre have a website. We will use images of children on our website to provide information, and to promote services available, to children and

families. In addition the work of the Research base is promoted and used to advertise a wide range of professional development courses.

I agree to images of my child(ren) featuring in the Integrated Centre website:

Yes/No*

Public Relations - Occasionally the local and national press approach us to take photographs/filming as part of any current news stories relating to very young children and their families. We will make every effort to inform you of when this may be happening in order that you are aware that images of your child may be published/used in external media sources.

I agree to my child(ren) being photographed and/or filmed for use in public relations exercise which may be available both on and offline.

Yes/No*

Social Media (including Twitter, Facebook, Instagram) – the Integrated Centre have accounts with social media sites. They are an invaluable way of sharing information quickly with parents about services available and also promoting parent-led activities at the Integrated Centre.

I agree to images of my child(ren) being posted online and I understand that the images will be in the public domain. I understand that if I do not like the image used I can request it be deleted but that the Integrated Centre cannot control how far it may already have been viewed.

Yes/No*

*Please delete as appropriate.

Signed: _____

Name: _____

Relationship to the child: _____

Email Address (if applicable): _____

Date: _____

Reviewed documentation and consent given on subsequent Home Visit or as part of the transition to a new setting within the Integrated Centre.

I continue to give my consent as stated above:

Signed: _____ -

Name: _____

Relationship (if different individual to the above);-----

Date: _____ -

Form B - Consent for Images within the Groupwork Programme

Images for Marketing, Social Media and Website

At Pen Green we regularly use digital photography and video to document children's learning. We take the utmost care to ensure that your child's wishes are respected and that only positive images of you and your child are displayed only with yours and their agreement. We particularly like the images attached and would like to use this and other similar images in the future.

I am happy for images of me and my child to be shared and shown...

	Yes	No
On Social Media	☐	☐
On the Pen Green Website	☐	☐
Marketing Materials	☐	☐

Name of child: _____

Name of parent / carer: _____

Signed (parent / carer): _____

Date: _____

By signing this form you give us permission to use images taken for the above purposes. If at any point you would like to withdraw this permission, please let us know.

If you would like to view future images before they are used please provide an email address and we will only use these images once we have received email notification from you.

Please email me with all images ☐

Email address _____

Form C Consent for Film/Photography - Staff, Volunteers & Governors

Within the Integrated Centre we regularly use staff images for a wide variety of purposes to promote the work of the setting which includes information for parents and carers, staff development and professional training, including our 'Meet the Teams' photo sheets for new workers at their induction, the role of the Governing Body, and ongoing promotion of the Centre services through social media.

To comply with the GDPR (2018) principles the Integrated Centre is required to seek your consent to continue to use your image in the areas illustrated above. Images may be used based on internal and external use and by completing the section below you can choose in which areas you would like your image to be featured.

If you have any further queries regarding this, please discuss this with your supervisor and/or the Data Protection Lead in the first instance

Full name:.....

Domain:.....

*I agree to my image being used for **internal** staff induction and training use. **Yes/No****
*I agree for my image to be used for Integrated Centre displays. **Yes/No****

Website –We will use images of staff, volunteers, and governors on our website to provide information, and to promote services available, to children, families and students. In addition the work of the Research base is promoted and used to advertise a wide range of professional development courses.

*I agree to my image featuring in the Integrated Centre website: **Yes/No****

Public Relations - Occasionally the local and national press approach us to take photographs/filming as part of any current news stories relating to very young children and their families. .

*I agree to my image being used and/or filmed for use in public relations exercise which may be available both on and offline. **Yes/No****

Social Media (including Twitter, Facebook, Instagram) – the Integrated Centre has accounts with social media sites. They are an invaluable way of sharing information quickly with parents about services available and promoting parent-led activities at the Integrated Centre.

*I agree to my images) being posted online and I understand that the images will be in the public domain. I understand that if I do not like the image used I can request it be deleted but that the Integrated Centre cannot control how far it may already have been viewed. **Yes/No****

Signed:.....

Date:.....

Form C.1 Consent for Film/Photography - Students & Activity Participants (Research Base)

Within the Integrated Centre we regularly use students, staff, volunteer and governors' images for a wide variety of purposes to promote the work of the setting which includes information for parents and carers, students, staff development and professional training. This includes our course/activity cohort photo sheets for all new students/participants at their induction and/or activity and the ongoing promotion of the Centre services through a variety of media.

In order to comply with the GDPR (2018) principles the Integrated Centre is required to seek your consent to use, and to continue to use, your image in the areas illustrated above. Images may be used on the basis of internal and external use and by completing the section below you can choose in which areas you would like your image to be featured.

If you have any further queries regarding this please discuss this with your course administrator and/or your Tutor/Facilitator in the first instance

Full name:..... Cohort/Activity:.....

*I agree to my image being used for **internal** student induction and training use.*

Yes/No*

I agree for my image to be used for Integrated Centre displays. **Yes/No***

Website – We will use images of students, staff, volunteers and governors on our website to provide information, and to promote services available, to children, families and students. In addition the work of the Research base is promoted and used to advertise a wide range of professional development courses.

I agree to my image featuring in the Integrated Centre website: **Yes/No***

Public Relations - Occasionally the local and national press approach us to take photographs/filming as part of any current news stories relating to very young children and their families. *I agree to my image being used and/or filmed for use in public relations exercise which may be available both on and offline.* **Yes/No***

Social Media (including Twitter, Facebook, Instagram) – the Integrated Centre has accounts with social media sites. They are an invaluable way of sharing information quickly with parents about services available and also promoting parent-led activities at the Integrated Centre.

I agree to my images) being posted online and I understand that the images will be in the public domain. I understand that if I do not like the image used I can request it be deleted but that the Integrated Centre cannot control how far it may already have been viewed. **Yes/No***

Signed:..... Date:.....

Incident Reporting

Filtering Change Log

All filtering change requests to be recorded by Network Administration or staff member authorised to adjust filtering levels. All filtering changes must be authorised by Network Administrator.

22 Linked documents: KCSIE 2025; www.ceop.police.uk/Safety-Centre; NNC Acceptable Use policy; Working Together to Safeguard Children

Website / category	Date	Requested by / reason	Authorised by	Change made by	Confirmed by	Date for review

Online Safety Incident Log

Details of ALL Online incidents to be recorded by staff and monitored monthly by the Network Administrator

Date of incident	Name of individual(s) involved	Device number/ location	Details of incident	Actions and reasons	Confirmed by

Filtering Change Log

All filtering change requests to be recorded by Network Administrator or staff member authorised to adjust filtering levels. All filtering changes must be authorised by the Network Administrator.

Website / category	Date	Requested by / reason	Authorised by	Change made by	Confirmed by	Date for review

Online Filtering Policy

The Network Administrator is authorised to make changes to internet filtering in relation to the Centre's broadband service.

23 Linked documents: KCSIE 2025; www.ceop.police.uk/Safety-Centre; NNC Acceptable Use policy; Working Together to Safeguard Children

How security is implemented

The Integrated Centre recognise they has a duty of care to protect any user from offensive material but also recognises that certain users, e.g. staff, undergraduate students, will require access to sites that may be unsuitable for children and families. The Centre has therefore created a list of automatically blocked websites deemed unsuitable for each group of users and 'banned words':

List of blocked sites & user groups

Process

1. If the site is on the banned list, a "site blocked" message is sent back to the user and access is denied.
2. If the site is not on the blacklist, access to the website is allowed.

Procedure for Blocking and Unblocking

Blacklists and 'banned word' lists are not exhaustive and there will be occasions when users discover unsuitable or inappropriate material originating from unblocked sources.

On the other hand, it may be considered that sites or accounts currently blocked should be unblocked.

The following procedures allow requests for blocking or unblocking to be dealt with promptly.

- Senior member of staff contacts Network administrator to request a website or email account to be blocked
- They investigate and if the request is non-contentious, contacts website provider to block the named site or account for specific or all user groups as appropriate. Blocking will normally take place immediately
- Provider adds this site to the black list and the site is then no longer available. A message on the users screen explains why this site is blocked, should any attempt be made to access it
- The procedure for requesting for a website or email account to be unblocked is broadly similar to the blocking procedure

Online Safety Incident Log

Details of ALL Online incidents to be recorded by staff and monitored monthly by the Network Administrator.

Date of incident	Name of individual(s) involved	Device number/location	Details of incident	Actions and reasons	Confirmed by

--	--	--	--	--	--

Online Log: Password Changes

Details of all occasions when network password has been changed to be recorded

Date	Reason for change (e.g. routine, security breach)	Authorised by	Change made by	Confirmed by	Date of next planned change