East Sussex County Council

St Thomas a Becket Nursery – Online Safety and Acceptable Use Policy

Date of last Review	Signed / Role	Date of next Review
February 2024		February 2025

Key Details:

Designated Safeguarding Leads: Amy Curtis, Nursery Manager; Clare Harrison, Nursery Lead

Contents

Important information

In personalising this online safety policy statement, we have also considered the following guidance documents:

- Keeping Children Safe in Education, 2023
- Relationships education (Primary)
- Teaching Online Safety in Schools: January 2023
- Meeting digital and technology standards in schools and colleges 2023
- Project Evolve
- Sharing nudes and semi-nudes: advise for education settings working with children and young people
- Keeping Children safe in out of school settings
- Resources on czone, to support primary schools with delivery of the Connected World

1. Policy Aims

- This online safety policy has been adapted by St Thomas a Becket Nursery involving staff, learners, Trustees and parents/carers, building on the East Sussex County Council/The Education People online safety policy template, with specialist advice and input as required.
- It takes account of the DfE statutory guidance Keeping Children Safe in Education 2023, Early Years and Foundation Stage and the East Sussex Safeguarding Children Partnership procedures.
- The purpose of this online safety policy is to:
    - Safeguard and protect all members of our community online.
    - Identify approaches to educate and raise awareness of online safety throughout the community.
    - Enable all staff to work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns.
- We identify that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:
    - **Content:** being exposed to illegal, inappropriate or harmful material
    - **Contact:** being subjected to harmful online interaction with other users
    - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
    - **Commerce/Contract:** risks such as online gambling, inappropriate advertising, phishing and or financial scams and sextortion (online sexual coercion and extortion of children).

2. Policy Scope

- We believe that online safety is an essential part of safeguarding and acknowledge its duty to ensure that all learners and staff are protected from potential harm online.
- We identify that the internet and associated devices, such as computers, tablets, mobile phones, smart watches and games consoles, are an important part of everyday life.
- We believe that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the Trustees, practitioners, support / admin staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as “staff” in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.
- T#he nursery will deal with such incidents within this policy and associated behaviour and anti-bullying policies to such extent as is reasonable and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that has taken place out of nursery. Action can only be taken over issues covered by the published Behaviour Policy

2.1 Links with other policies and practices

This policy **links** with several other policies and activities including:

- British Values delivery
- Code of conduct/staff behaviour policy including social media
- Confidentiality / Sharing Information policy
- Managing Behaviour Positively policy
- Safeguarding and Child protection policy, including mobile phones
- Curriculum delivery, such as: Personal Social and Health Education (PSHE)
- Data security and retention
- Image use procedures

2.2 Online safety in extracurricular activities provided by an external organisation

- If our nursery engages community groups, sports associations and service providers to run extra-curricular activities, we ensure that appropriate arrangements are in place to keep children safe.
- We seek assurances that where services or activities are provided separately by another body (not under direct supervision or management of our nrsery staff) that there are appropriate safeguarding and child protection policies and procedures in place (including online safety) and will inspect these as necessary. This applies regardless of whether or not the children who are attending these services are on our nursery roll.
- Safeguarding arrangements would be clearly detailed in any transfer of control agreement (i.e. lease or hire agreement).
- The DfE has published *Keeping Children Safe during community activities, after-school clubs and tuition* for organisations and individuals who provide these activities for children and young people and this document contains a section on online safety which makes clear that the provider should have an online safety policy or acceptable use policies in place as well as appropriate filtering and monitoring. A staff behaviour policy should also include information on relationships and communications between children (and parents) and staff/volunteers, including the use of social media.

3. Monitoring and Review

- Technology in this area evolves and changes rapidly; We will review this policy at least annually
    - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor our ICT use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Manager will be informed of online safety concerns, as appropriate.

- The Nursery Lead will report on a regular basis to the Trustees on all Safeguarding safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) Nursery Manager – Amy Curtis, has lead responsibility for online safety.
    - Whilst activities of the designated safeguarding lead may be delegated to appropriately trained deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL.
- We uphold the need for a key responsible person as identified in the 'The digital and technology standards in 'schools guidance', and assign the Nursery Manager for ensuring our ICT safety standards are met'. We will report on Safeguarding to the Trustees every term.
- We recognise that all members of our nursery and the wider community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team and Trustees will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure that online safety is a running and interrelated theme whilst devising and implementing the whole nursery approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies (including the staff code of conduct and/or acceptable use policies) and considering online safety whilst planning curriculum activities, any practitioner training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.
- Ensure that we are doing all that they reasonably can to limit children's exposures to risks from the nursery's IT useage. We have appropriate filtering and monitoring systems in place. We will have an awareness and understanding of the provisions in

place and will work with our contracted ICT company to monitor and renew the safety and security of our systems and networks.

- Ensure that all relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively as well as knowing how to escalate concerns when identified.
- Ensure that we regularly review the effectiveness of filters and monitoring systems; as we increasingly work online, knowing that it is essential that children are safeguarded from potentially harmful and inappropriate online material (including when they are online at home).
- Ensure that the DfE's filtering and monitoring standards for schools and colleges are being met: this will be supported through using the checklist appended to this policy.
- Ensure that online safety is embedded within a progressive preventative curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Recognise that effective education will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs or disabilities.
- Ensure that ALL members of staff receive regular, updated, and appropriate online safety training which is integrated, aligned and considered as part of the whole school safeguarding approach and know how to escalate concerns when identified.
- Support the DSL and any deputies by ensuring they have the additional time, funding, training, resources and support they need to carry out the role effectively.
- Ensure there are robust reporting channels for the nursery community to access regarding online safety concerns, including internal, local and national support.
- Audit and evaluate online safety practice, annually, to identify strengths and areas for improvement.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology that considers and reflects the risks our children face.
- Communicate with parents regarding the importance of children being safe online and how to keep children safe
- Communicate with parents about Tapestry and safe sharing of information of this platform.

4.2 The Designated Safeguarding Lead (DSL) will:

- Be the Nursery Manager and the Nursery Lead.
- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside the Nursery deputies to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Liaise with all staff on matters of safeguarding that include online and digital safety.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety, including filtering and monitoring and have the relevant knowledge and up to date training required to keep learners safe online
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns to the Nursery Lead and the Trustees.
- Work with the Nursery Lead to review and update online safety policies on a regular basis (at least annually) with national and County guidance and including children's voice.
- Meet at least termly with the Nursery Lead for safeguarding discussions, including online safety.

4.3 It is the responsibility of all members of staff to:

- Be aware that technology is a significant component of many safeguarding and wellbeing issues and that children are at risk of abuse online as well as face to face and that in many cases abuse will take place concurrently via online channels and in daily life.
- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use expectations within the Staff Code of Conduct.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Proactively monitor the use of digital technologies, tablets, cameras etc and consistently implement current policies with regard to these devices
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Ensure that children and their parents are guided to access only sites checked as suitable for children's use and that processes are in place for dealing with behaviours or disclosures indicating children's access to any unsuitable material in the home environment.
- Reinforce the school's online safety messages when teaching lessons online

4.4 It is the responsibility of the nursery leadership team to ensure the safety of the technical environment:

- We access professional technical support to provide a safety perspective to the DSL and leadership team, especially in the implementation of appropriate online safety procedures which comply with DfE's filtering…standards for [schools and colleges] an educational environment.
- Implement appropriate security measures to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised. All nursery devices are protected by the school's firewall and additionally are encrypted and password protected. Children are only able to access approved, downloaded content on our nursery tablets.
- Report any filtering breaches to the DSL and Nursery Lead, as well as, the settings Internet Service Provider, Univserve.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL or Nursery Lead.

4.5. It is the responsibility of nursery staff to support all children (at a level that is appropriate to their individual age and ability) to:

- Engage in age-appropriate safe online educational opportunities provided by the nursery.
- Contribute to the development of online safety policies by understanding how to keep themselves and their friends safe.
- Read and adhere to Acceptable Use Policies, which are appended to the end of this policy.
- Understand the importance of good online safety practice out of nursery and understand that this policy covers actions outside of nursery.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.

- Seek help from a trusted adult or other support services, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

- Read the Acceptable Use Policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the Acceptable Use Policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as Tapesty or any learning platforms / network resources that we may introduce at a given time, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with learners

- We will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible online behaviour at nursery and at home by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in Personal, Social, Health and Economic (PSHE) and any use of apps or in sharing images and information through Tapesty.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating children in the safe use of the internet.

    - Teaching children to tell an adult about any images that make them feel uncomfortable.
- We will support children to understand the Acceptable Use Policies in a way which suits their age and ability by:
    - Displaying age-appropriate acceptable use posters in all rooms with internet access.
    - Rewarding positive use of technology.
    - Providing online safety education through age appropriate information as part of the transition from Caterpillars to Butterflies and for school readiness.
    - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

5.2 Vulnerable Learners

- We recognise that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- We recognise that children with cognitive difficulties may be unable to understand the difference between fact and fiction in online content and then may repeat the content/behaviours without understanding the consequences of doing so.
- We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners and their families through providing support and guidance where we see fit.
- When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate, including the SENCO or Social Worker for any Child in Care.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with ALL members of staff as part of induction.

- Provide updates for Trustees and up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates within *existing safeguarding and child protection training/updates.*
- This will cover the potential risks posed to learners (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored (through the school), and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- We recognise that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
- Providing information and guidance on online safety in a variety of formats.
    - This will include signposting to parent guidance websites, offering specific online safety awareness training where available and highlighting online safety at other events such as one to ones and through newsletters.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.

- Requesting that they read online safety information as part of joining our nursery, requiring them to read our acceptable use policies and discuss the implications with their children.
- Providing information about our link to school's filtering and monitoring as well as information about ways that children can be kept safe online.

6. Responding to Online Safety Incidents and Concerns

- All members of the nursery community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth produced sexual imagery (sharing of nudes or semi-nudes/sexting), cyberbullying and illegal content.
- All members of the nursery community will be directed to the DSL or headteacher in such circumstances.
- All members of the nursery community must respect confidentiality and the need to follow the official procedures for reporting concerns.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- Safeguarding concerns and incidents, at level 3 or 4 on the Continuum of Need, will be reported to Single Point of Advice in line with East Sussex Safeguarding and Child Protection model policy.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice from the Standards and Learning Effectiveness Service Safeguarding Team.
- Where there is suspicion that illegal activity has occurred contact the Sussex Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our nursery community (for example if other local settings are involved or the public may be at risk), the DSL will contact Sussex Police first to ensure that potential investigations are not compromised.

6.1 Concerns about Learners' Welfare

- The DSL (or deputies) will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL (or deputies) will record these issues in line with our child protection policy.
- The DSL (or deputies) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the East Sussex Safeguarding Children Partnership thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

6.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Nursery Lead and Nursery Manager in accordance with the Whistleblowing Policy.
- For any allegations regarding a member of staff's online conduct a consultation will be sought with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

7. Procedures for Responding to Specific Online Incidents or Concerns

7.1 Child-on-child online sexual violence and sexual harassment

Our setting has accessed and understood part 5 of Keeping Children Safe in Education September 2023.

- We recognise that sexual violence and sexual harassment between children can take place online and our staff will remain vigilant and report any concern where one of our

nursery children may be targeted. Examples may include; sharing of images /videos, threats, unwanted comments on social media, and online sexual exploitation.

    - We will respond to concerns relating to images of our children or displays of sexualised behaviours, violence or harassment between children in line with our Safeguarding and Child Protection Policy.

- We recognise that the internet brings a serious and lasting potential for the impact of any these concerns to extend further than the local community, and for a victim (or alleged perpetrator) to become marginalised and excluded by online communities.
- We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- We will ensure that all members of the nursery community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment, of and between children, by implementing a range of age appropriate teaching as part of our PSHE curriculum.
- If we suspect that any child is at risk, wherever this takes place, we will:
    - Immediately notify the DSL and act in accordance with our child protection policies.
    - Provide the necessary safeguards and support for all nursery community, such as offering specific advice on blocking and reporting online content.
    - If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police.
    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, the DSL will discuss this with Sussex Police first to ensure that investigations are not compromised.

7.2 Youth Produced Sexual Imagery ('Sharing nudes and semi nudes')

- We recognise youth produced sexual imagery (known as "sharing nudes and semi nudes") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL.
- If we suspect that any child is at risk, wherever this takes place, we will not:
  view any images suspected of being youth produced sexual imagery. We will:
    - Immediately notify the DSL and act in accordance with our child protection policies, refer the matter to SPOA and also ensure our response falls in line with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people, guidance.
    - Provide the necessary safeguards and support for all nursery community, such as offering specific advice on blocking and reporting online content.
    - If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police.
    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, the DSL will discuss this with Sussex Police first

7.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation and County Lines)

- We will ensure that all members of the nursery community are aware of online child sexual abuse including exploitation and grooming, the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.

- We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the nursery community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the nursery community is aware of the 'Click CEOP' report button for a child to use if something has happened online which has made them feel unsafe, scared or worried.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our child protection policies and the relevant East Sussex Safeguarding Child Partnership's procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Care (if required/ appropriate) and immediately inform the police via 101 (or 999 if a child is at immediate risk)
    - Carry out a risk assessment which considers any vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.

    - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Police.
- If children at other settings are believed to have been targeted, the DSL will contact the Police.

7.4 Indecent Images of Children (IIOC)

- We will ensure that all members of the nursery community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet service provider (ISP) which implements appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the Police.
- If made aware of IIOC, we will:
    - Act in accordance with our Safeguarding and Child Protection Policy.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as Sussex police or the LADO.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the DSL is informed, who will investigate the incident.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the setting provided devices, we will:
    - Ensure that the DSL and Nursery Lead are informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted once directed to by the police.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
    - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
    - Ensure that the Nursery Lead and Nursery Manager is informed in line with our Whistle Blowing Policy which confirms procedures for managing allegations against staff.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff procedures.
    - Quarantine any devices until police advice has been sought.

7.5 Cyberbullying

- All staff will understand that children are capable of abusing their peers online. Cyberbullying, along with all other forms of bullying, will not be tolerated and will be dealt with in full discussion with families of children involved.

7.6 Cybercrime

- We will ensure that all members of the community are aware that children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.
- If there are concerns about a child in this area, the DSL will consider referring into the Cyber Choices programme.
- We will seek advice from Cyber Choices, 'NPCC- When to call the Police' and National Cyber Security Centre.

7.7 Online Hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at our setting and will be responded to in line with existing policies.
- All members of the community are advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Standards and Learning Effectiveness Service and/or Sussex Police.

7.8 Online Radicalisation and Extremism

- We will ensure that all members of the nursery community are made aware of the role of the internet as a tool for radicalisation
- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site through the school firewall and filtering and via our encrypted devices.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our Safeguarding and Child Protection Policy.

- If we are concerned that a member of staff or Trustee may be at risk of radicalisation online, the Nursery Lead and Manager will be informed immediately, and action will be taken in line with the child protection and allegations policies.

8. Safer Use of Technology

8.1 Nursery Use

We use a range of technology. This includes access to:

  - tablets and apps
  - Digital cameras
- All devices will be used in accordance with our Acceptable Use Policies and with appropriate safety and security measures in place. Children do not have direct access to the internet.
- Members of staff will always evaluate websites, tools and apps fully before use or recommending for use at home.
- The nursery will promote the use age-appropriate search tools [following East Sussex Guidance], to identify safe *search tools for families use. Examples include SWGfL Swiggle, Dorling Kindersley find out, Google Safe Search or CBBC safe search.*
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of children will be appropriate to their age and ability - Access to the internet will be though adult prepared downloads only of approved online materials and apps, which support the learning outcomes planned for the learners age and ability.

8.2 Managing Internet Access

- All staff will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

8.3 Filtering and Monitoring

- The nursery fall within St Thomas A Becket school's [compliant with the DfE] filtering and monitoring standards.

A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found at: UK Safer Internet Centre: appropriate filtering and monitoring.

The appended checklist will be used as a guide to ensure our compliance with the filtering and monitoring good practice.

8.3.1 Decision Making

- We have ensured that our setting has age and ability appropriate filtering and monitoring and use in place, to limit learner's exposure to online risks.
- We are aware of the need to prevent "over blocking" but limit use of internet access at nursery.
- Filtering and monitoring has been informed by the school risk assessment. A review will also be carried out following the identification of a safeguarding risk or any changes in working practice who follow the guidance outlined in the DfE filtering and monitoring standards when carrying out the review.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective management and teaching about safe and responsible use is essential.

8.3.2 Decision Making

- Education broadband connectivity is provided through ST Thomas a Becket School who block sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- We work with ST Thomas a Becket Primary School and Uniserve South East to ensure that our filtering facility is continually updated.

- If we discover unsuitable sites, we will:
    - turn off the monitor/screen and report the concern immediately to the DSL.
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL and school.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Sussex Police or CEOP.

8.3.3 Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is also monitored through the school who review internet and web access.
- If a concern is identified via monitoring approaches we will be notified and the concern will be investigated following Safeguarding, Whistle Blowing and Disciplinary procedures
- Staff are informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

8.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation, our safe practice and our Information Sharing Policy.

8.5 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
    - Protecting all devices through the school software firewall
    - Ensuring all nursery devices have their security features enabled, correctly configured and up to date

- Ensuring that accounts only have the access that they require to perform their role and are authenticated to access data and services, such as My Concern
- Virus protection being updated regularly.
- Encryption for personal data received and sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network
- The appropriate use of user logins and passwords to access our network.
- All users are expected to log off or lock their screens/devices if systems are unattended.

8.5.1 Password Policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- We require all users to:
  - Use strong passwords for access into our system.
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Not to login as another user at any time.

8.6 Managing the Safety of our Website

- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.

- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website is through our website provider and Nurery Lead and is secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

8.7 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

8.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
    - The forwarding of any chain messages/emails is not permitted.
    - Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately inform Amy Curtis, Nursery Manager or Clare Harrison, Nursery Lead if they receive offensive communication, and this will be recorded in our safeguarding files/records.

8.8.1 Staff Email

- The use of personal email addresses by staff for any official setting business is not permitted.
    - All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.
  The nursery may consider using 1:1 video call sessions to support interventions with children such as long term absences from nursery.
- These sessions will only be provided where they have been risk assessed and approved by The Nursery Lead and Manager and parental consent given.
- Where the communication with an individual child takes place, there will be two adults involved; this will provide a safeguard for the adults and the children.
- These two adults will either be physically in the same room, with the second member of staff being referenced to the child so that they are aware, or, where staff are working remotely, they will both be within the virtual room of the meeting.
- In either case both adults will be present before the child is admitted to the online session.

8.9 Management of Applications (apps) used to Record Children's Progress (if used)

- We use Tapestry to track learners progress and share appropriate information with parents and carers.
- The Nursery Manager is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

- To safeguard learner's data:
    - Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
    - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

9. Social Media

9.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of our nursery community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of our nursery community are expected to engage in social media in a positive, safe and responsible manner.
    - All members of our community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others or that could damage the reputation of the nursery or individual within it.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site.
    - The use of social media on nursery equipment for personal use is not permitted.

    - Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary action.
- Concerns regarding the online conduct of any member of our nursery community on social media, must be reported to the DSL and will be managed in accordance with our Whistle Blowing - allegations against staff, behaviour and Safeguarding and Child Protection policies.

9.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our Code of Conduct.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.

    - Keeping passwords safe and confidential and using two factor authentication wherever possible.
    - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of our setting on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with children and families

- Communication with children both in the offline world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web cams and other hand-held devices. (Given the ever-changing world of technology it should be noted that this list gives examples only and is not exhaustive.) Staff should not request or respond to any personal information from children. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour'.
- Staff should not give out any personal contact details.
- On school trips, staff should have a school mobile phone rather than having to rely on their own device.
- Staff should not accept friend requests from families, past or present. If a member of staff feels that this is necessary, they should first seek guidance from the DSL or Nursery Lead. Any pre-existing relationships or exceptions that may compromise this, will be discussed

with DSL and/or the Nursery Lead (see *Staff Behaviour Policy/ Code of Conduct for further information*)

- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the headteacher/manager.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputies).

9.3 Learners' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age-appropriate sites and resources.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including behaviour and Acceptable Use Policies.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning expected underage viewing or use of social media sites / games and the sharing of inappropriate images or messages that may be considered threatening, hurtful or defamatory to others.
- Children will be taught in age appropriate language and detail:
    - To consider the risks of sharing personal details on social media sites which could identify them and/or their location.
    - The importance of only talking to known friends on social media and to make profiles private.
    - Not to make any online friends without a parent/carer or other responsible adult's permission.
    - To use safe passwords and two factor authentication where possible.
    - To use social media sites which are appropriate for their age and abilities.
    - To tell an adult about unwanted communications.

9.4 Official Use of Social Media (Only include if setting has official social media)

- Our official social media channels are:
  Website and Facebook
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
    - The official use of social media as a communication tool has been risk assessed and approved by the Nursery Lead.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    - Official social media sites are suitably protected and, linked to/from our website.
    - Public communications through the website, Mailchimp or Tapestry on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including image/camera use, data protection, confidentiality and child protection.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Expectations of Staff

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Sign our social media acceptable use policy.
    - Always be professional and aware they are an ambassador for the setting.
    - Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of the setting.
    - Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace including libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Not share images on the official social media channel without explicit, written consent from families.
    - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, learners, parents and carers.
    - Inform their line manager, the DSL and the Nursery Lead of any concerns, such as criticism, inappropriate content or contact from learners.

10. Use of Personal Devices and Mobile Phones

We recognise that personal communication through mobile technologies is an accepted part of everyday life for staff and parents/carers, but technologies must be used safely and appropriately within the setting.

The Use of mobile phones or smartphone watches is not permitted in the children's rooms.

10.1 Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, Safeguarding and Child Protection and Staff Code of Conduct.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - We accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of our community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in areas where any children are present.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the nursery community; any breaches will be dealt with as part of our disciplinary policy.
    - All members of our nursery community are expected to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or Safeguarding and Child Protection policies.

10.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant Safeguarding and Child Protection policy and procedures.
- Staff are advised to:
    - Keep mobile phones and personal devices in a safe and secure place away from the children's areas.

  - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled when in the nursery setting.
  - Not use personal devices whilst with the children unless written permission has been given by the Nursery Manager, such as in emergency circumstances.
  - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are discouraged from using their own personal phones or devices for contacting families.
  - Any pre-existing relationships, or emergency situations which could undermine this, will be discussed and approved with the DSL
- Staff will not use personal devices:
  - To take photos or videos of children and will only use work-provided equipment for this purpose.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct, allegations procedures and disciplinary policy
  - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

10.3 Visitors' Use of Personal Devices and Mobile Phones

- Visitors are not permitted to use personal devices when in rooms where children are present.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL of any breaches our policy.

11. Useful Links for Educational Settings

01323 463026
childcare.support@eastsussex.gov.uk

If you are concerned about a child in East Sussex contact SPOA (Single Point of Advice) on 01323 464222 or 0-19.SPOA@eastsussex.gov.uk

Standards and Learning Effectiveness Service (SLES):
SLES.Safeguarding@eastsussex.gov.uk

East Sussex Support and Guidance for Educational Settings
https://czone.eastsussex.gov.uk/safeguarding/

East Sussex Safeguarding Children Partnership
www.sussexchildprotection.procedures.org.uk/

Sussex Police: www.sussex.police.uk

For non-urgent Police contact 101.

If we think the child is in immediate danger, you we will call the police on 999.

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
  - https://www.childnet.com/what-we-do/our-projects/thrive-online/
  - https://www.childnet.com/resources/connect-with-respect-send/
- Project Evolve: https://projectevolve.co.uk/
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: Net-Aware
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- Get Safe Online: www.getsafeonline.org
- Action Fraud: www.actionfraud.police.uk
- Online Safety Toolkit: Online Safety - Czone (eastsussex.gov.uk)

National Links and Resources for Professionals/Parents/Carers:

National Crime Agency's CEOP Education Programme: Protecting children andyoung people from online child sexual abuse through education

12. Linking our Online Safety Policy with other nursery policies.

This online safety policy is used as part of an effective whole nursery approach to online safety. We understand our responsibilities to ensure that children are able to use the internet appropriately and safely. This online safety policy is recognised as a safeguarding policy, and falls within the role and responsibilities the Designated Safeguarding Lead (DSL).

This policy links with other relevant Child Protection and Safeguarding policies, Managing Behaviour Positively For Children's Wellbeing and Staff Code of Conduct. Acceptable Use is expected as key theme running through our Safeguarding practices.

13. Disclaimer

Acceptable Use Agreement for Staff and Volunteers

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

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

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

For my professional and personal safety I must understand that:

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

For the safety of others:

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

For the safety of the group / setting, I understand that:

- I will not try to access anything illegal, harmful or inappropriate
- It is my responsibility to immediately report any illegal, harmful or inappropriate incident
- I will not share my online personal information (e.g. social networking profiles) with the children and young people in my care
- I will not deliberately bypass any systems designed to keep the nursery safer
- I will only transport, hold, disclose or share personal information about myself or others, as allowed by the Data Protection Policy of the nursery. Where personal data is transferred, externally, it must be encrypted
- I understand that Data Protection Policy requires that any personal data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by the group's / setting's policy to disclose such information to an appropriate authority
- Personal passwords and those of other users will always be confidential

- I will not download anything that I do not have the right to use
- I will only use my personal device if I have permission and use it within the agreed rules
- I will inform the appropriate person if I find any damage or faults with technology
- I will not attempt to install programmes of any type on the devices belonging to the group, without permission

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

Staff / Volunteer name:
Signed:
Date:

Acceptable Use Agreement for Children

The Nursery Agreement

This agreement is intended to help our children understand how to stay safe while using the internet and other digital technologies for educational, personal and recreational use.

Children's Declaration - this is how we stay safe when we use computers:

- I will ask an adult if I want to use a phone or tablet and will only use it when they are with me;
- I will ask for help from an adult if I am not sure what to do or if I think I have pushed some wrong buttons
- I will tell an adult if I see something that worries or upsets me on the screen
- I won't talk or video message anyone or send photos on the phone or tablet unless my mummy or daddy have told me that it is ok to do so
- I will always be kind to people I am talking to on the phone or tablet

For Older Children who are learning from home:

- *I will ask an adult if I want to use a computer or device;*
- *If I am in a 'live lesson' with my nursery or teacher an adult will be close by me;*
- *I will make sure that I use my computer or device in a shared space, (not in my bedroom);*
- *I will only do activities online that a teacher or suitable adult has told me or allowed me to use;*
- *I will ask for help from an adult if I am not sure what to do or if I think something has gone wrong;*
- *I will tell a teacher or adult if I see something that upsets me on the screen or if I am worried or unsure about something;*

Childs Name:

Parents Name:
Parents Signature:

Date:

Letter to Parents/carers for Early Years

Dear Parents and Guardians,

As part of their learning and development, your child will have the opportunity to access a range of digital technologies, including Early Years appropriate educational games and apps on the nursery tablets, and by various digital technologies at home. We recognise the value of using these digital technologies and the potential risks involved and therefore have rigorous online safety policies and procedures in place which are available to read on our website.

During any time of Remote Home Learning your child will also have the opportunity to access digital technology at home, as they do at nursery. We recognise the value of using these digital technologies, but also the potential risks involved.

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

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

Signed:

Amy Curtis

Nursery Manger

Acceptable Use of Technology Template Statement and Forms for Parents/Carers

- I have read – and discussed with my child the pupil Acceptable Use of Technology Agreement Policy (AUP) for St Thomas a Becket Nursery and understand that this AUP will help keep my child safe online;
- I understand that the AUP applies to my child's use of nursery devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns;
- I am aware that the use of nursery devices and systems may be monitored for safety and security reason to keep my child safe. This monitoring will take place in accordance with data protection, privacy, and human rights legislation.
- I understand that my child needs a safe and appropriate place to access remote learning if my child has an extended period away from nursery. I will ensure my child's access to remote learning is appropriately supervised. When accessing video learning, I will ensure they are in an appropriate location (e.g. not in a bedroom) and that they are suitably dressed
- I give permission for my child to submit work and upload work related videos to their teacher;
- I understand that the school/setting will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school/setting devices and systems. I understand that the school/setting cannot ultimately be held responsible for the nature and content of materials accessed on the internet or if my child is using their own mobile technologies
- I give permission for my child's work to be used on nursery Social Media Account;
- I am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the nursery community.
- I understand that the school/setting will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety.

- I will inform the nursery or other relevant organisations if I have concerns over my child's or other members of the nursery communities' safety online.
- I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of nursery.
- I will support the nursery online safety approaches and will discuss this agreement and the pupil agreement with my child. I will use appropriate parental controls and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Childs Name:

Parents Name:

Parents Signature:

Date:

Meeting digital technology standards in schools

Filtering and monitoring standards **Task/responsibility**	**Notes**
Identifiede and assigned roles and responsibilities:	
Responsibility: Nursery Manager **Task:** Identify and confirm with the school that annual checks are carried out on filtering and monitoring of internet use.	
Responsibility: Nursery Lead **Task**: Ensure any reports of breaches are fully investigated	
Responsibility: Joint **Task:** Understand the risk profile of pupils – incl. Children Looked After, SEND, EAL	
Responsibility: SLT **Task**: All staff have received appropriate and up to date training and understand their role	
Responsibility: SLT **Task**: All staff follow policies and procedures and processes around online safety and filtering and monitoring	
Responsibility: SLT **Task**: All staff act on reports and concerns	
Responsibility: DSL **Task**: Oversee and act on safeguarding concerns	
Responsibility: ITSP **Task**: Complete actions following concerns or checks to systems	
Responsibility: Joint **Task**: Outside safeguarding influences that should be considered - e.g. county lines, vulnerable adult criminal exploitation	
Responsibility: Joint **Task**: Does the PSHE curricula cover age appropriate discussions	
Responsibility: Joint **Task**: How are devices used within school? (e.g. BYOD)	
Responsibility: Joint **Task**: What related safeguarding and technology policies are in place?	
Responsibility: Joint **Task**: What checks are in place – how are resulting actions handled?	
Responsibility: Joint **Task**: Does filtering and monitoring work on new devices? Is this checked before they are given to staff/pupils?	

Questions to School	**Notes**
Responsibility: DSL and ITSP **Task**: Are you blocking access to adult content?	
Responsibility: DSL and ITSP **Task**: Is filtering applied to any device which connects to the school broadband connection?	
Responsibility: DSL and ITSP **Task**: Can filtering handle multilingual content, images, misspellings, abbreviations?	
Responsibility: DSL and ITSP **Task**: Does filtering work on mobile devices? *Is there evidence, have you checked?*	
Responsibility: DSL and ITSP **Task**: Does filtering work on app content? *Is there evidence, have you checked?*	
Responsibility: DSL and ITSP **Task**: Will the filtering system identify the IP address, device name and ID and where possible the individual who has attempted to access unsuitable or illegal content?	
Responsibility: ITSP **Task**: Are IT staff given safeguarding training including online safety training?	
Responsibility: ITSP **Task**: Are IT staff reporting any issues (safeguarding concerns to the DSL)?	