



E-Safety Policy

Inc. Use of Mobile Devices, IT agreement forms & Use of AI A6

**Dolphin School Trust
inc. Noah's Ark Nurseries**

Reviewed by:	Lucy Price (Headteacher)
Last reviewed:	October 2026
Next review:	October 2027

1. Introduction

Dolphin School Trust recognises that technology plays an increasingly important role in education, communication and everyday life. We are committed to providing a safe, supportive and stimulating environment in which children can develop the knowledge, skills and confidence to use technology responsibly.

Online safety is an integral part of the Trust's safeguarding responsibilities and is embedded within its Christian ethos and values of Love, Wisdom and Truth. We aim to equip children to make wise choices, treat others with kindness and respect, recognise potential risks and seek help when necessary.

The Trust recognises that effective online safety extends beyond technical safeguards. It requires strong leadership, appropriate policies and procedures, staff training, pupil education, parental partnership, effective filtering and monitoring, and regular review.

This policy applies across Dolphin School and Noah's Ark Nurseries, including Reception, The Harbour and the nursery settings.

It applies to all staff, governors, contractors, agency workers, volunteers and pupils, as appropriate, when using Trust systems, devices or online services. Relevant provisions also apply to visitors and to school-related online activity outside the premises.

This policy has been developed with reference to:

- Keeping Children Safe in Education 2026.
- The Education (Independent School Standards) Regulations 2014.
- The Department for Education's Mobile Phones in Schools statutory guidance (2026).
- The DfE Filtering and Monitoring Standards, updated September 2026.
- Current DfE guidance on generative artificial intelligence in education and AI product safety.
- The Early Years Foundation Stage statutory framework.
- The UK General Data Protection Regulation and Data Protection Act 2018.
- The Equality Act 2010.
- Relevant UK Council for Internet Safety guidance.

2. Aims and Principles

The Trust aims to:

- Provide a safe digital environment for children and staff.
- Promote responsible, respectful and age-appropriate use of technology.
- Protect pupils from harmful or inappropriate online content and contact.
- Equip pupils to recognise and respond to online risks.
- Ensure appropriate filtering, monitoring and technical safeguards are in place.
- Establish clear expectations for the use of school and personal devices.
- Support the safe and responsible introduction of emerging technologies, including artificial intelligence.
- Protect personal information, privacy and confidentiality.
- Ensure online safeguarding concerns are recognised, recorded and responded to promptly.
- Work in partnership with parents to promote positive digital habits and online safety beyond school.

- Provide appropriate additional support for pupils with SEND or other vulnerabilities.

Online safety is a shared responsibility, with safeguarding leadership and oversight provided by the Designated Safeguarding Lead (DSL), Headteacher and governors.

3. Roles and Responsibilities

Headteacher

The Headteacher has overall responsibility for ensuring that online safety arrangements are implemented effectively across the Trust.

This includes ensuring that appropriate resources, training, risk assessments, technical safeguards and reporting arrangements are in place.

The Headteacher is the Senior Responsible Owner for filtering and monitoring and receives regular information about the effectiveness of the Trust's systems.

Designated Safeguarding Lead

The DSL has lead responsibility for online safety, including oversight of filtering and monitoring arrangements.

The DSL is responsible for:

- Ensuring online safety concerns are recognised and addressed in accordance with the Child Protection and Safeguarding Policy.
- Reviewing relevant filtering and monitoring alerts.
- Working with IT support to identify emerging risks and potential weaknesses.
- Ensuring safeguarding incidents involving technology are recorded appropriately.
- Supporting staff training and awareness.
- Liaising with external safeguarding agencies where necessary.
- Contributing to the annual review of online safety and filtering and monitoring arrangements.

The DSL at Dolphin School is **Adam Woodcraft**. Appropriate designated safeguarding arrangements are maintained across Noah's Ark Nurseries.

IT Support

The Trust's IT contractor is responsible for the technical operation, maintenance and security of the network, devices, filtering and monitoring systems.

This includes supporting software updates, security controls, system testing and the investigation of technical concerns.

The Trust currently uses Senso and FortiCloud as part of its filtering and monitoring arrangements.

Governors

Governors/proprietors provide oversight of online safety, ensuring that appropriate arrangements are in place and that identified concerns and risks are addressed.

The safeguarding governor receives information about filtering and monitoring, significant incidents, training and review outcomes.

Staff

All staff are responsible for maintaining safe and professional digital practice.

Staff must:

- Follow this policy and the Trust's Acceptable Use Agreements.
- Supervise pupils appropriately when technology is being used.
- Report online safeguarding concerns promptly.
- Protect confidential information and school systems.
- Use approved devices, software and communication channels.
- Maintain professional boundaries online.
- Participate in relevant training.

4. Conditions of Use and Acceptable Use

The Trust provides IT equipment and systems to support teaching, learning, administration and the effective operation of the School and Nurseries.

These facilities are provided primarily for authorised professional and educational purposes.

All users are expected to use technology responsibly, lawfully and in a manner consistent with the Trust's ethos and safeguarding responsibilities.

Staff and pupils must comply with the relevant Acceptable Use Agreement.

Account Security

Users must use their own authorised accounts and must not access another person's account without permission.

Passwords must be kept secure and must not be shared with other users. Any suspected compromise must be reported promptly.

Staff must lock devices when unattended and ensure that confidential information cannot be viewed by unauthorised individuals.

Appropriate Use

Users must not:

- Access, create, share or distribute unlawful, abusive, discriminatory, extremist or otherwise inappropriate material.
- Engage in cyberbullying, harassment, intimidation or threatening behaviour.
- Attempt to bypass filtering, monitoring or other security arrangements.
- Access another person's files, accounts or personal information without authorisation.
- Install unauthorised software, applications or browser extensions.
- Introduce malicious software or deliberately compromise the Trust's systems.
- Use school technology in a manner that places children, staff or the Trust at risk.
- Use AI or other digital technologies to create misleading, harmful or inappropriate material.

Staff must use approved school email accounts and communication systems for school-related correspondence.

Personal email accounts and unauthorised messaging services must not be used for school business.

5. E-Safety Education and Training

Pupil Education

Online safety is taught through the curriculum and reinforced through assemblies, Relationship Time, classroom discussion and other appropriate opportunities.

Teaching is age-appropriate and reflects the needs and developmental stages of pupils.

The curriculum addresses the four categories of online risk:

Content: Exposure to harmful, inappropriate or misleading information, images and media.

Contact: Risks arising from communication or interaction with other people online.

Conduct: Risks associated with an individual's own online behaviour and its impact on others.

Commerce: Risks involving financial exploitation, scams, inappropriate advertising and other commercial activity.

Pupils are taught to:

- Protect personal information and passwords.
- Communicate respectfully and responsibly.
- Recognise and report cyberbullying.
- Understand the risks of sharing photographs, videos and personal information.
- Evaluate the reliability of online information.
- Recognise misleading content, misinformation and online manipulation.
- Understand that online actions can have lasting consequences.
- Seek help from a trusted adult when something online causes concern.

The Trust recognises that online risks evolve rapidly. Teaching will be reviewed and adapted to reflect emerging technologies and safeguarding concerns.

Artificial Intelligence and Digital Literacy

Pupils will develop an age-appropriate understanding of artificial intelligence and its increasing presence in everyday digital environments.

Teaching will help children understand that AI-generated information may be inaccurate, misleading or biased, and that images, audio and video may be artificially created or manipulated.

Pupils will be encouraged to think critically about information, question the reliability of digital sources and understand the importance of producing their own work.

Pupil use of generative AI applications will be permitted only where specifically approved, age-appropriate and supervised by staff.

Staff Training

All staff receive online safety information as part of induction and are expected to familiarise themselves with this policy and the relevant Acceptable Use Agreement.

Ongoing training and reminders will address:

- Online safeguarding risks.
- Filtering and monitoring responsibilities.
- Safe use of school systems and devices.
- Cybersecurity and data protection.
- Professional conduct and boundaries.
- Responding to online incidents.
- Emerging risks, including artificial intelligence.

The Trust will also seek to provide parents with information and opportunities to develop their understanding of online safety.

6. Professional Behaviour and Online Conduct

Staff are expected to maintain appropriate professional standards in their use of technology, both within and outside school.

Personal online activity must not compromise safeguarding, confidentiality, professional boundaries or the Trust's reputation.

Staff must not disclose confidential information about pupils, parents, colleagues or school matters through personal social media or other public platforms.

Staff must not communicate privately with current pupils through personal social media accounts, personal messaging applications or other unauthorised channels.

Staff should not accept or initiate personal social media connections with current pupils. Any unusual or concerning contact should be reported to the Senior Team or DSL.

Staff should ensure that their personal social media activity is clearly distinguishable from official Trust communications and must not present personal opinions as the views of the Trust.

Where staff have existing personal or family relationships with parents, professional boundaries and confidentiality requirements continue to apply.

The Trust recognises that staff are entitled to a private life. Any concerns relating to personal online activity will be considered proportionately, taking account of professional responsibilities and safeguarding obligations.

7. Network Security and School Devices

The Trust maintains appropriate technical and organisational safeguards to protect its IT systems, devices and information.

These include access controls, passwords, filtering and monitoring, software updates and secure storage arrangements.

Staff must report suspected security breaches, lost devices, compromised accounts, malicious software or inappropriate access to information promptly.

Use of School Devices

School laptops, Chromebooks, tablets and other devices must be used responsibly and protected from loss, damage and unauthorised access.

Devices taken off-site remain subject to the Trust's policies.

Staff must not leave school devices unattended in public places or unsecured vehicles.

Confidential information must not be downloaded onto personal devices or stored using unauthorised external storage services.

Where remote access is necessary, staff must use approved systems and follow the Trust's data protection and security arrangements.

Pupils may use school devices only for authorised educational purposes and under appropriate supervision.

Software and Applications

New software, applications, browser extensions or digital services must be approved before installation or use.

Approval will consider educational value, technical compatibility, security, data protection and safeguarding risks.

Where applications process personal information, appropriate checks and assessments must be completed before use.

8. Filtering and Monitoring

The Trust recognises filtering and monitoring as essential components of its safeguarding arrangements.

Filtering systems are intended to prevent access to harmful or inappropriate online material, while monitoring systems help identify concerning activity or potential safeguarding risks.

The Trust uses Senso and FortiCloud as part of its current arrangements.

Filtering and monitoring apply to devices using the Trust's networks, including personal devices connected to those networks, subject to the technical capabilities and lawful scope of the systems.

School-managed devices used away from the premises will be subject to appropriate safeguards, including remote filtering where supported.

Pupils must not attempt to circumvent filtering or monitoring through VPNs, mobile hotspots, tethering or other methods.

Responsibilities and Oversight

The DSL receives and reviews relevant safeguarding alerts and works with IT support to investigate concerns.

The Headteacher receives regular monitoring information and oversees the effectiveness of the arrangements.

IT support maintains the technical systems and advises on emerging risks and necessary improvements.

Teaching staff remain responsible for active supervision of pupils when technology is used. Filtering and monitoring do not replace appropriate adult supervision.

Review and Testing

The Trust undertakes an annual written review of filtering and monitoring, involving the DSL, Headteacher and IT support, with findings reported to governors.

Arrangements will also be reviewed following significant changes to technology, identified weaknesses or safeguarding incidents.

The Trust undertakes an online safety risk assessment, taking account of the four categories of online risk: Content, Contact, Conduct and Commerce.

AI-Related Risks

Filtering and monitoring arrangements will take account of risks associated with generative AI, AI-enabled search engines, chatbots and applications capable of generating text, images, audio or video.

Before introducing a new AI-enabled platform for pupil use, the Trust will consider its educational purpose, age suitability, content safeguards, privacy arrangements and monitoring capabilities.

Where concerns or weaknesses are identified, appropriate action will be taken and documented.

9. Mobile Phones, Smartwatches and Personal Devices

Pupil Mobile Phones

Dolphin School operates a mobile phone-free school day in accordance with the Department for Education's statutory guidance.

Pupils must not use personal mobile phones during the school day, including lessons, breaktimes, lunchtimes, clubs and school-supervised activities, unless an individual exception has been expressly authorised.

Where pupils need to bring a mobile phone to school, it must be switched off and handed to their class teacher on arrival for secure storage. Phones may be collected at the end of the school day.

Pupils must not retain or use mobile phones during the day without authorisation.

Parents who need to contact their child urgently should do so through the School Office. Pupils who need to contact their parents will be supported by staff.

Smartwatches and Wearable Devices

Restrictions also apply to personal smartwatches and other wearable devices with communication, internet, camera or recording capabilities.

Such devices must not be used to communicate, record, photograph or access online services during the school day.

The School may require these devices to be switched off or securely stored.

Individual Exceptions

The Headteacher may authorise an individual exception where necessary to meet a pupil's disability, medical or other exceptional needs.

Any arrangement will be documented, proportionate and communicated to relevant staff.

Breaches

Breaches of the mobile phone and smart device rules will be addressed proportionately under the Behaviour Policy.

Any searching, screening or confiscation will follow applicable legislation and current DfE guidance.

Staff Personal Devices

Staff must comply with the Trust's separate Staff Mobile Phone and Smart Device Use Policy.

Personal devices must not be used for routine personal communication while supervising pupils.

The Trust provides school mobile phones for emergency use during educational visits, off-site activities and other appropriate circumstances.

Where personal devices are exceptionally required for operational reasons, this must be authorised and appropriate safeguarding safeguards maintained.

Staff must not use personal devices to photograph, video or record pupils.

10. Photography, Video and Safe Use of Images

The Trust recognises the educational and community value of photographs and video while acknowledging the importance of protecting children's privacy and safety.

Photographs and recordings of pupils must be taken using authorised school devices and stored securely within approved systems.

Staff must not use personal mobile phones or personal cameras to capture images of pupils.

Parental Permissions

Parents are asked to provide permissions for specified uses of their child's image, including internal school activities, publications, publicity and online communication.

The Trust maintains records of these permissions, and staff must check the relevant information before taking or using photographs.

Parents may withdraw consent for consent-based uses at any time.

Internal educational uses of images and external promotional uses may rely on different lawful bases. The Trust will identify and document the appropriate basis for each purpose and provide clear information to parents.

Images must not be published in a manner that unnecessarily identifies children or compromises their safety.

The Trust will not routinely publish pupils' full names alongside their photographs.

Storage and Sharing

Images must be stored securely within authorised school systems and accessed only by those with a legitimate professional need.

Staff must not transfer images to personal accounts, unauthorised cloud storage or personal removable devices.

Any suspected unauthorised sharing or loss of images must be reported promptly.

AI-Generated or Manipulated Images

Staff and pupils must not use AI tools or other applications to create, alter or distribute misleading, inappropriate or harmful images of members of the school community.

Identifiable images or recordings of pupils must not be uploaded to AI applications without specific Trust approval and appropriate safeguarding and data protection checks.

11. Particular Considerations for E-Safety in the Early Years Foundation Stage

This section applies to Reception classes at Dolphin School and both Noah's Ark Nursery settings.

The Trust recognises the increasing influence of digital technology on young children's learning, development and everyday experiences. The use of technology within the Early Years Foundation Stage (EYFS) must reflect the Trust's Christian ethos and commitment to providing a safe, nurturing and stimulating environment.

Particular consideration is given to both the direct and indirect impact of technology on children's learning, development, relationships and wellbeing.

11.1 Teaching and Learning

Technology may be used to enhance children's learning, creativity, communication and understanding of the world.

Digital resources should be carefully selected to ensure they are age-appropriate, educationally purposeful and consistent with the developmental needs of young children.

The Trust recognises that technology should complement, rather than replace, opportunities for play, exploration, physical activity, practical experiences and meaningful interaction with adults and other children.

Children will be introduced to simple principles of online safety in ways appropriate to their age and understanding, including recognising when something makes them uncomfortable and knowing to seek help from a trusted adult.

11.2 Screen Use

In accordance with the EYFS statutory framework, the Trust will have regard to the Department for Education's guidance on screen use in early years settings.

Screen-based activities must have a clear educational purpose and should be balanced with active, practical and social learning experiences.

Staff will consider the duration, content and purpose of screen use, ensuring that children are actively engaged rather than routinely exposed to passive screen-based entertainment.

Screen use will be appropriately supervised, and staff will consider the individual developmental, communication and sensory needs of children.

Screens must not be used routinely as a substitute for adult interaction, play, behaviour support or emotional regulation.

11.3 Professional Use of Technology

Early Years staff use approved digital systems to support assessment, observations, individual learning plans, communication with parents and administrative responsibilities.

These may include Tapestry, Engage and other approved Trust systems.

Digital record-keeping must be proportionate and should not unnecessarily reduce the time staff spend interacting with and supporting children.

All information must be recorded, stored and shared securely in accordance with the Trust's safeguarding and data protection procedures.

11.4 Personal Mobile Phones and Smart Devices

Staff must not use personal mobile phones in EYFS classrooms, outdoor play areas, changing areas or while supervising children.

Personal mobile phones must be kept in locked boxes, the staffroom or another designated secure area during contact time with children.

Staff may use personal mobile phones only in authorised areas during breaks and never in areas where children are present.

These restrictions also apply to personal smartwatches, wearable devices and other electronic equipment with imaging, recording or sharing capabilities.

Personal devices must never be used to photograph, film or record children.

11.5 Photography, Video and Digital Observations

Photographs and recordings of children must be taken only using authorised Trust devices.

Images used for observations, assessment, learning records or communication with parents must be stored and shared through approved systems, in accordance with safeguarding, data protection and parental permission arrangements.

Staff must not transfer photographs or recordings to personal devices, personal email accounts or unauthorised storage services.

Images and recordings must be limited to those reasonably necessary for legitimate educational, assessment or communication purposes.

11.6 Emergency and Off-Site Communication

In an emergency, staff should use the school or nursery landline or an agreed Trust mobile phone.

Where the use of a personal mobile phone is exceptionally necessary, including during an educational visit, this must be authorised by the Headteacher or designated senior leader.

Any authorised use must be restricted to the agreed purpose and must not involve personal photography, recording or inappropriate communication.

11.7 Visitors, Volunteers and Contractors

Visitors, volunteers and contractors must comply with the Trust's restrictions on mobile phones, cameras and other personal electronic devices while in EYFS areas.

Personal devices must not be used to photograph, film or record children.

Staff are responsible for ensuring that visitors understand the relevant safeguarding expectations and that any concerns are reported promptly.

11.8 Safeguarding and Reporting Concerns

Any inappropriate use of technology, suspected breach of device restrictions or concern involving images, recordings or online communication must be reported promptly to the Designated Safeguarding Lead.

Concerns will be recorded and managed in accordance with the Trust's Child Protection and Safeguarding Policy.

11.9 Designated E-Safety Leads

The designated e-safety leads for the Early Years settings are:

Noah's Ark Nursery, Dolphin: Mr Adam Woodcraft

Noah's Ark Nursery, West Side: Mrs Rachael Strachan

These individuals support the implementation of online safety procedures within their respective settings and work in conjunction with the Trust's safeguarding leadership.

11.10 Partnership with Parents

The Trust recognises the importance of working with parents to support safe, balanced and age-appropriate use of technology.

Staff will share appropriate guidance and advice with parents where relevant, including the importance of supervision, suitable content, healthy screen-use habits and the protection of children's personal information.

The Trust will seek to model positive digital practice and support families in developing children's confidence and safety in an increasingly digital world.

12. Inclusion and Pupils with SEND

The Trust recognises that pupils with SEND may experience additional online vulnerabilities or require adaptations to access technology safely and effectively.

Staff will consider pupils' individual needs when planning digital activities, including the use of assistive technology, communication tools and online learning resources.

Additional explanation, visual support, supervision or adapted teaching may be provided where appropriate.

For pupils attending The Harbour, online safety teaching and digital activities will be adapted to their developmental needs, communication profiles and individual support arrangements.

The Trust will ensure that safeguarding measures do not unnecessarily prevent pupils with SEND from benefiting from appropriate technology and reasonable adjustments.

13. Responding to Online Safety Incidents

All online safety concerns must be taken seriously and responded to proportionately.

Staff who become aware of inappropriate online material, cyberbullying, suspected grooming, harmful communication, unauthorised sharing of images or other concerning activity must report the matter promptly.

Where a concern relates to the safety or welfare of a child, it must be reported to the DSL or a Deputy DSL in accordance with the Child Protection and Safeguarding Policy.

Immediate Action

Staff should take appropriate steps to protect children from further exposure to harmful material or contact.

Where necessary, access to a device, account or service may be temporarily restricted.

Staff must not investigate safeguarding concerns beyond their responsibilities or unnecessarily access, copy or circulate potentially harmful or illegal material.

Concerns involving nude or semi-nude images of children must be handled in accordance with current safeguarding guidance, including restrictions on viewing, copying, forwarding or deleting such material.

Recording and Referral

Safeguarding incidents must be recorded in the Trust's approved safeguarding system.

Technical incidents, including security breaches or filtering failures, must be reported to the appropriate IT support personnel.

Where necessary, the DSL will consult or refer to relevant external agencies, including children's social care, the police, the local authority or other appropriate services.

Pupil Misuse

Where a pupil has misused technology, the School will consider the nature and seriousness of the incident, the child's age and understanding, any safeguarding concerns and relevant SEND needs.

Responses may include discussion, education, parental involvement, increased supervision, temporary restrictions on technology use or sanctions under the Behaviour Policy.

The Trust will prioritise safeguarding and education alongside proportionate disciplinary responses.

Staff Misuse

Suspected staff misuse will be addressed in accordance with the Staff Code of Conduct, Child Protection and Safeguarding Policy and Disciplinary, Grievance and Capability Procedures, as appropriate.

Where allegations meet the relevant safeguarding thresholds, the Trust will follow the applicable procedures for allegations against adults, including referral to the LADO where required.

14. Monitoring, Privacy and Data Protection

The Trust may monitor the use of its IT systems, accounts, networks and devices for legitimate safeguarding, security, operational and compliance purposes.

Any monitoring or access to communications will be carried out lawfully, transparently and proportionately, with appropriate authorisation and regard for individuals' privacy rights.

Staff and pupils will be informed about relevant monitoring arrangements through policies, privacy notices and acceptable-use information.

Personal information must be processed in accordance with UK GDPR, the Data Protection Act 2018 and the Trust's Data Protection Policy.

Sensitive or confidential information may be shared externally only where there is a legitimate purpose, appropriate authority and suitable security arrangements.

Records of online safety incidents will be retained in accordance with the Trust's Records Retention Schedule and safeguarding requirements.

15. Breaches of Policy

Breaches of this policy will be considered in light of their nature, seriousness, circumstances and potential impact.

For pupils, the response will follow the Behaviour Management Policy and relevant safeguarding procedures.

For staff, breaches may be considered under the Trust's Disciplinary, Grievance and Capability Procedures, Staff Code of Conduct or safeguarding procedures, as appropriate.

Serious incidents may result in restrictions on system access, formal disciplinary action or referral to external agencies where required.

Any investigation or disciplinary action will follow appropriate procedures and principles of fairness and proportionality.

Complaints relating to online safety will be addressed through the Trust's Complaints Policy, except where safeguarding or other specific procedures take precedence.

16. Review and Related Policies

This policy will be reviewed annually, or sooner where significant changes to legislation, guidance, technology or safeguarding risks make this necessary.

The review will consider emerging online threats, filtering and monitoring effectiveness, reported incidents, staff training needs and developments in artificial intelligence.

This policy should be read alongside the Trust's:

- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Staff Mobile Phone and Smart Device Use Policy
- Behaviour Management Policy
- Anti-Bullying Policy
- Data Protection Policy
- Communications Policy
- SEND Policy
- Educational Visits Policy
- Disciplinary, Grievance and Capability Procedures

Appendices – Dolphin School & Noah’s Ark Nurseries E-Safety Policy

Appendix	Item
Appendix 1	Safe and Responsible use of AI in School
Appendix 2	Social Media guidelines
Appendix 3	Staff Acceptable Use Agreement - IT, Online Safety and Artificial Intelligence
Appendix 4	Additional Acceptable Use Agreement - PE, Dance and Music Staff
Appendix 5	Acceptable Use Agreement for Upper School Pupils
Appendix 6	Acceptable Use Agreement for Lower School Pupils
Appendix 7	Incident form to report IT misuse
Appendix 8	Parental permission form for image consent

Appendix 1 – Safe and Responsible Use of Artificial Intelligence

1. Introduction

Dolphin School Trust recognises that artificial intelligence offers opportunities to enhance teaching, learning, administration and staff wellbeing.

AI can support resource creation, lesson planning, differentiation, administrative efficiency and the development of digital literacy.

However, the Trust also recognises risks relating to safeguarding, privacy, inaccurate information, bias, inappropriate content and overreliance on automated systems.

The Trust is committed to introducing AI responsibly, ensuring that technology supports rather than replaces professional judgement, human relationships and high-quality teaching.

2. Objectives

The Trust's approach to AI aims to:

- Enhance educational experiences where AI offers demonstrable benefits.
- Reduce unnecessary staff workload.
- Promote responsible and ethical use.
- Protect pupils, staff and families from potential harm.
- Ensure compliance with safeguarding and data protection requirements.
- Maintain transparency and accountability.
- Support inclusion and equitable access to technology.

3. Approval of AI Applications

Staff may use AI applications for school purposes only where they have been approved by the Senior Team.

The Trust maintains a register of approved AI tools.

Before approving a new application, the Senior Team will consider:

- The proposed educational or operational purpose.
- Potential benefits and limitations.
- Safeguarding and age-appropriateness.
- Data protection and privacy implications.
- Information security.
- Accessibility and inclusion.
- The provider's arrangements for content moderation and user safety.
- Whether appropriate training and oversight are available.
- Financial and contractual considerations.

Relevant data protection assessments, including a DPIA where required, will be completed before the application is introduced.

Approval may be restricted to specified purposes, groups of users or types of information.

4. Staff Use of AI

AI may be used to support appropriate professional tasks, including:

- Lesson planning and curriculum development.
- Producing and adapting teaching resources.
- Generating ideas for classroom activities.
- Creating model texts and examples.
- Supporting administrative tasks.
- Developing appropriate differentiated materials.
- Summarising non-confidential information.
- Supporting professional development.

Staff remain responsible for all material they produce or use, regardless of whether AI has contributed to its creation.

AI-generated content must be checked for accuracy, suitability, bias, copyright considerations and relevance to pupils' needs.

Staff must not present unverified AI-generated information as fact.

AI must not replace teachers' professional judgement or their knowledge of individual children.

5. Protection of Personal and Confidential Information

Staff must not enter identifiable pupil, parent or staff information into AI applications unless the specific use has been approved and the necessary data protection safeguards are in place.

Particular care must be taken with:

- Safeguarding records.
- SEND and EHCP documentation.
- Medical information.
- Behaviour records.
- Assessment information.
- Family circumstances.
- Staff employment information.
- Photographs, recordings and other identifiable material.

The Trust will identify an appropriate lawful basis for processing personal information and ensure that relevant privacy, security and contractual requirements are met.

Where processing is likely to result in high risk to individuals, a Data Protection Impact Assessment must be completed.

AI tools must not be used to process confidential information merely because doing so would be convenient or save time.

6. AI and Educational Decision-Making

AI may support the analysis of information and the generation of suggestions, but it must not replace appropriate professional assessment.

Staff must not rely solely on AI-generated outputs when making significant decisions about a child's:

- Academic attainment or progress.

- SEND or support requirements.
- Behaviour.
- Wellbeing or mental health.
- Safeguarding needs.
- Educational placement or future provision.

Professional judgement, appropriate assessment and human oversight must remain central to such decisions.

Any proposed use of AI to support significant decisions about individuals must receive specific approval and appropriate legal and data protection scrutiny.

7. Pupil-Facing AI Applications

Pupil-facing AI tools may include adaptive learning platforms, educational games, intelligent tutoring systems and other applications designed to support learning.

Such tools will be introduced only where they are age-appropriate, educationally justified and subject to suitable safeguards.

The Trust will consider whether the tool:

- Complies with relevant age restrictions.
- Provides appropriate content moderation.
- Protects personal information.
- Allows effective adult supervision.
- Avoids inappropriate or manipulative interactions.
- Supports healthy cognitive, social and emotional development.
- Meets the needs of pupils with SEND.
- Offers clear educational benefits.

Direct pupil interaction with open-ended generative AI systems will not be permitted without specific approval and appropriate supervision.

8. Academic Integrity and Responsible Use

The Trust encourages pupils to develop independent thinking, creativity and pride in their own work.

AI must not be used to misrepresent the authorship of work, fabricate evidence or avoid learning activities.

Where AI use is permitted, staff will explain how it may be used and when its contribution should be acknowledged.

Pupils will be taught that AI-generated information may contain errors and should be checked against reliable sources.

9. AI-Generated Images, Audio and Video

The Trust recognises the safeguarding risks associated with AI-generated and manipulated media, including deepfakes, impersonation and misleading or inappropriate content.

Staff and pupils must not use AI to create or distribute harmful, sexualised, discriminatory, threatening or misleading representations of members of the school community.

Images, audio or video identifying pupils must not be uploaded to AI services without specific approval and appropriate safeguards.

Any suspected misuse involving AI-generated media must be reported promptly to the DSL.

10. Staff Training and Professional Development

Staff will receive appropriate information and training on the safe, effective and ethical use of AI.

Training will address:

- The capabilities and limitations of AI.
- Safeguarding risks.
- Accuracy, bias and misinformation.
- Data protection and confidentiality.
- Appropriate classroom use.
- Professional accountability.
- Emerging developments and relevant DfE guidance.

Staff are encouraged to share effective practice and raise concerns about tools that may be unsuitable or unsafe.

11. Transparency and Communication

The Trust will communicate appropriately with parents, pupils and governors about significant uses of AI in education and school operations.

Where AI applications directly affect pupils' learning or involve processing personal information, the Trust will provide appropriate information about their purpose and safeguards.

Governors will receive relevant updates about AI adoption, associated risks and the effectiveness of oversight arrangements.

12. Monitoring and Review

Approved AI applications will be reviewed periodically to ensure that they remain educationally beneficial, secure and appropriate.

The Senior Team will consider feedback from staff and other relevant stakeholders, changes in technology and developments in national guidance.

Approval may be withdrawn where an application no longer meets the Trust's expectations or presents unacceptable risks.

The Senior Team retains responsibility for overseeing the Trust's approach to AI, working with the DSL, IT support and data protection advisers as appropriate.

Appendix 2 - Social Media Guidelines

Dolphin School Trust, incorporating Noah's Ark Nurseries

1. Purpose and Ethos

Official Trust social media accounts are used to celebrate school life, communicate the Trust's identity and provide an insight into the education and community experienced by pupils and families.

Content should reflect the Trust's Christian ethos and values of Love, Wisdom and Truth, presenting Dolphin School and Noah's Ark Nurseries as nurturing, joyful and ambitious educational communities.

These guidelines apply to the management of official Trust accounts and set out expectations for appropriate social media engagement by staff, pupils and parents.

They should be read alongside the E-Safety Policy, Safeguarding and Child Protection Policy, Staff Code of Conduct, Communications Policy and Data Protection Policy.

2. Official Accounts and Responsibilities

Official Trust social media accounts may be created, managed and accessed only by authorised members of staff.

The Headteacher and Senior Team will oversee the Trust's social media presence, including arrangements for content approval, account security and appropriate engagement.

Staff responsible for managing official accounts must:

- Use approved Trust accounts and secure login arrangements.
- Ensure access is restricted to authorised individuals.
- Use Trust-owned or otherwise specifically authorised devices and systems.
- Ensure content is accurate, appropriate and consistent with the Trust's ethos.
- Check relevant photographic permissions before publication.
- Avoid disclosing confidential information or unnecessarily identifying pupils.
- Report any account compromise, inappropriate communication or safeguarding concern promptly.

Access permissions will be reviewed when staff responsibilities change or employment ends.

3. Content, Images and Publication

Official social media content should celebrate the breadth of school life, including learning, achievements, events, enrichment opportunities and community relationships.

All public-facing content must be approved in accordance with arrangements established by the Senior Team.

Photographs and recordings of pupils must be taken using authorised Trust devices and managed in accordance with Section 10 of the E-Safety Policy.

Before publication, staff must check the relevant parental permissions recorded by the Trust.

Pupils' full names should not routinely appear alongside photographs, and content must not disclose sensitive personal information or information that could compromise a child's safety.

Images of pupils in swimwear, changing areas or other sensitive circumstances must not be published.

AI-generated or manipulated images must not misrepresent pupils, staff or school activities. Identifiable images of pupils must not be uploaded to AI applications without specific Trust approval and appropriate safeguards.

4. Comments, Messaging and Interaction

Official social media accounts are intended for communication and community engagement, not for confidential correspondence or individual pupil matters.

Comments and direct messaging functions will be disabled, restricted or appropriately moderated.

Where messages are received concerning admissions, complaints, safeguarding or individual pupils, staff should redirect the matter to the appropriate official communication channel.

Social media must not replace SchoolPost, approved school email, Evolve or other established Trust communication systems.

Abusive, discriminatory, threatening or inappropriate comments may be hidden, removed or reported, with safeguarding concerns referred promptly to the Designated Safeguarding Lead.

5. Staff Personal Social Media Use

Staff are entitled to a private life and personal use of social media. However, they must maintain appropriate professional boundaries and protect the confidentiality, dignity and safety of members of the Trust community.

Staff must not:

- Communicate privately with current pupils through personal social media accounts or messaging services.
- Share confidential information about pupils, families, colleagues or Trust operations.
- Publish photographs or recordings of pupils obtained through their professional role on personal accounts.
- Present personal views as official statements of the Trust.
- Engage in online behaviour that compromises safeguarding responsibilities or professional standards.

Where staff have existing family or personal relationships with parents, appropriate professional boundaries and confidentiality requirements continue to apply.

Concerns will be considered proportionately under the relevant safeguarding, Staff Code of Conduct or disciplinary procedures.

6. Parent and Carer Use of Social Media

The Trust values the positive contribution of parents and carers in celebrating school life and supporting the school community.

Parents and carers are asked to:

- Respect the privacy of other children and families when sharing photographs, videos or information online.
- Avoid publishing identifiable images of other people's children without appropriate permission.
- Refrain from sharing confidential or sensitive information relating to pupils, staff or families.
- Communicate respectfully and avoid personal criticism, harassment or inappropriate comments directed at members of the school community.
- Raise concerns through the Trust's established communication and complaints procedures rather than through public social media discussions.

Parent-organised WhatsApp groups and other informal online groups are independent of the Trust and are not official communication channels.

The Trust encourages those participating in such groups to communicate respectfully, maintain confidentiality and avoid sharing unverified or sensitive information.

Where concerns arise, the Headteacher may contact those involved, request removal of inappropriate content or take other proportionate steps within the Trust's authority.

7. Pupil Use of Social Media

Pupils are taught about responsible online communication, privacy, cyberbullying, misinformation and the importance of seeking help from trusted adults.

Pupils must not access personal social media accounts during the school day or use Trust devices to access unauthorised social media platforms.

Any educational use of social media content must be age-appropriate, approved and supervised by staff.

Pupils must not contact staff through personal social media accounts.

The Trust will reinforce relevant platform age restrictions and encourage parents to support age-appropriate digital use at home.

Concerns involving cyberbullying, harmful content, inappropriate contact or other online risks will be addressed through the E-Safety, Safeguarding and Child Protection, Anti-Bullying and Behaviour Management Policies, as appropriate.

8. Safeguarding, Monitoring and Review

Any social media activity that raises a safeguarding concern must be reported promptly to the DSL and recorded through the Trust's established safeguarding procedures.

Technical or account security concerns must also be reported to the appropriate IT support personnel.

The Headteacher and Senior Team will oversee the Trust's official social media arrangements, including account access, publication procedures and responses to inappropriate interactions.

These guidelines will be reviewed annually alongside the E-Safety Policy, or sooner where changes in technology, safeguarding risks or relevant guidance make this necessary.

Appendix 3:

Staff Acceptable Use Agreement – IT, Online Safety and Artificial Intelligence

(google form link [here](#))

This agreement applies to all staff working across Dolphin School and Noah's Ark Nurseries, including teaching, support, administrative, specialist, temporary and agency staff where appropriate.

By signing this agreement, I confirm that I have read and understood the Trust's E-Safety and Online Safety Policy and agree to the following responsibilities.

Responsible and Professional Use

- I will use Trust technology, accounts and systems responsibly and in accordance with my professional role.
- I will use only approved school communication channels for school-related correspondence with pupils, parents and colleagues.
- I will maintain professional boundaries in all online communication and social media activity.
- I will not access, create or distribute inappropriate, discriminatory, offensive or unlawful material.
- I will respect copyright and intellectual property rights.

Safeguarding and Confidentiality

- I will protect confidential information about pupils, families, staff and the Trust.
- I will not share personal or sensitive information through unauthorised applications, personal accounts or insecure systems.
- I will report any online safeguarding concern promptly to the Designated Safeguarding Lead.
- I will not use personal devices to photograph, film or record pupils.
- I will use approved Trust devices and systems for photographs, observations and recordings, ensuring that relevant permissions and safeguards are followed.

Security and School Devices

- I will keep my login credentials secure and will not share my account with unauthorised users.
- I will lock devices when unattended and take appropriate precautions when using school equipment away from the premises.
- I will not install unauthorised software, applications or browser extensions.

- I will report suspected security breaches, lost devices, inappropriate material or filtering concerns promptly.
- I understand that the Trust may monitor the use of its systems and devices for legitimate safeguarding, security and operational purposes, in accordance with applicable law and Trust policies.

Mobile Phones and Smart Devices

- I will comply with the Trust's Staff Mobile Phone and Smart Device Use Policy.
- I will not use personal mobile phones or smart devices for personal communication while supervising children.
- I understand that additional restrictions apply in EYFS settings, including secure storage of personal devices during contact time.
- I will use Trust-provided devices for school-related communication wherever required and will seek authorisation for any exceptional arrangements.

Artificial Intelligence

- I will use only AI tools approved by the Trust for school purposes.
- I will not enter confidential or identifiable pupil, parent or staff information into AI applications without specific authorisation and appropriate safeguards.
- I will check the accuracy, suitability and fairness of AI-generated content before using it.
- I understand that AI may support, but must not replace, my professional judgement or responsibility.
- I will report any safeguarding, privacy or security concerns arising from AI use.

Declaration

I understand that failure to comply with this agreement may result in restrictions on access to Trust systems and action under the relevant safeguarding or disciplinary procedures.

I confirm that I have read and understood this agreement and agree to comply with its requirements.

Staff name: _____

Role: _____

Signature: _____

Date: _____

Appendix 4:

Additional IT Acceptable Use Agreement – PE, Dance and Music Staff

(google form link [here](#))

This agreement supplements the Trust's Staff Acceptable Use Agreement and applies to specialist staff who may require access to mobile devices for legitimate professional purposes.

I understand that the Trust recognises the practical need for mobile devices in certain circumstances, including sports fixtures, off-site activities, music lessons, dance sessions and performances.

I agree that:

- I will use a Trust-provided device wherever practicable.
- Where authorised, I may retain or use a personal mobile phone for essential professional purposes, including urgent fixture arrangements, travel logistics or communication relating to school activities.
- Where authorised, I may use a mobile device to play music during lessons, assemblies, clubs or performances.
- I will keep any personal device out of sight of pupils wherever practicable and will not use it for personal communication while supervising children.
- I will not use a personal device to photograph, film or record pupils.
- I will not communicate directly with pupils or parents through personal messaging applications, social media or personal email accounts.
- I will follow the Trust's safeguarding, data protection and educational visits procedures.
- I understand that these exceptions do not override the additional restrictions applying within EYFS settings.
- I will report any concerns, inappropriate communication or device-related incidents promptly.

I understand that any exception must be authorised by the Senior Team and may be reviewed or withdrawn.

Staff name: _____

Role: _____

Authorised arrangements (if applicable): _____

Staff signature: _____

Date: _____

Senior Team authorisation: _____

Appendix 5

Upper School Acceptable Use Agreement - Years 3-6

(Google Form link [here](#))

Using Technology Safely, Wisely and Kindly

At Dolphin, we use technology to learn, create, explore and communicate. We want everyone to feel safe, respected and supported when using technology.

I agree that:

Using Technology Responsibly

- I will use school Chromebooks, computers and other devices for learning and only when my teacher gives permission.
- I will use websites, applications and online resources approved by my teacher.
- I will not try to bypass school internet filters or access websites that are blocked.
- I will look after school equipment and report anything that is broken or not working properly.

Keeping Myself and Others Safe

- I will keep my password private and will not try to access another person's account.
- I will not share personal information, including my address, telephone number, passwords or photographs, without permission.
- I will use school email and messaging systems only as directed by my teacher.
- I will communicate kindly and respectfully and will not send messages that could hurt, embarrass or upset someone.
- I will not take, share or upload photographs, videos or recordings of other people without permission.
- I will tell a trusted adult straight away if I see something online that worries, frightens or upsets me, or if someone contacts me inappropriately.

Thinking Carefully Online

- I understand that not everything I see or read online is true.
- I will think carefully about whether information is reliable and ask for help if I am unsure.
- I will use artificial intelligence (AI) tools only when my teacher gives permission.
- I understand that AI can make mistakes and that I must check information carefully.
- I will be honest about my work and will not pretend that work created by AI or another person is entirely my own.

Mobile Phones and Smart Devices

- I will follow the School's rules about mobile phones, smartwatches and other personal devices.
- I understand that personal devices must not be used during the school day unless the School has specifically given permission.

My Promise

I understand that these rules help keep me and other people safe. If I make a mistake or something goes wrong online, I know that I can speak to a trusted adult and ask for help.

I understand that not following these rules may mean that my use of technology is restricted.

Pupil name: _____

Year group: _____

Pupil signature: _____

Date: _____

Class teacher signature: _____

Appendix 6:

Lower School Acceptable Use Agreement - Years 1-2

(Google Form Link [here](#))

My Promise to Stay Safe Online

At Dolphin, we use technology to help us learn and have fun.

I promise that:

1. **I will listen to my teacher** and only use technology when I am allowed to.
2. **I will be kind** when I use computers and send messages.
3. **I will keep my password safe** and will not use someone else's account.
4. **I will keep my information private** and will not share my address, phone number or photographs without permission.
5. **I will look after our devices** and use them carefully.
6. **I will ask before using new websites or apps**, including AI tools.
7. **I will remember that not everything online is true.**
8. **I will tell a grown-up straight away** if I see something that makes me worried, sad or uncomfortable.

If something goes wrong online, I can always ask for help.

I understand that these rules help keep everyone safe.

Pupil name: _____

Class: _____

Pupil signature: _____

Date: _____

Class teacher signature: _____

Appendix 7 – Online Safety and IT Misuse Incident Report Form

Including Dolphin School and Noah's Ark Nurseries

(Google Form link [here](#))

Confidential – To be completed by the member of staff reporting the incident and passed to the Designated Safeguarding Lead or appropriate member of the Senior Team.

Where an incident involves a safeguarding concern, staff must report it immediately in accordance with the Safeguarding and Child Protection Policy. This form does not replace the Trust's safeguarding recording procedures.

1. Incident Details

Name of staff member reporting: _____

Role: _____

School/Nursery setting: _____

Date of incident: _____

Time of incident: _____

Date and time reported: _____

Location of incident: _____

Is this an isolated or repeated incident? ☐ Isolated ☐ Repeated ☐ Unknown

If repeated, provide dates or approximate duration:

How was the incident identified?

- ☐ Directly witnessed by staff
- ☐ Reported by a pupil
- ☐ Reported by a parent/carers
- ☐ Identified through filtering or monitoring
- ☐ Reported by another member of staff
- ☐ Other: _____

2. Nature of the Incident

Tick all that apply.

- ☐ Access to inappropriate or harmful online content
- ☐ Cyberbullying, harassment or threatening communication
- ☐ Inappropriate online contact or communication
- ☐ Misuse of school devices, accounts or systems
- ☐ Attempt to bypass filtering or monitoring
- ☐ Unauthorised photography, video or recording
- ☐ Sharing or misuse of personal or confidential information
- ☐ AI-generated or manipulated content, including images or video
- ☐ Suspected account compromise or cybersecurity incident

- ☐ Inappropriate use of mobile phones or smart devices
☐ Other: _____

Individuals involved (names and roles, where known):

Relevant devices, applications, websites, accounts or services:

3. Description of Incident

Provide a factual account of what happened, including relevant dates, times, actions, communications and observations.

Distinguish between what was directly observed, what was reported by others and any information that remains unconfirmed.

What concerns have been identified?

Are any other individuals known or believed to be affected?

4. Immediate Action Taken

Tick all that apply.

- ☐ DSL or Deputy DSL informed
☐ Senior Team informed
☐ IT support contacted
☐ Access to a device, account or service restricted
☐ Device secured
☐ Relevant information or evidence secured appropriately
☐ Parent/carer contacted, where appropriate
☐ No immediate action required
☐ Other: _____

Details of actions taken, by whom and when:

Has relevant information been recorded and secured?

- ☐ Yes ☐ No ☐ Not applicable

Has any relevant device or equipment been secured?

☐ Yes ☐ No ☐ Not applicable

Name of person responsible:

Important: Staff must not unnecessarily view, copy, forward or download harmful or potentially illegal material. Any concern involving nude or semi-nude images of children must be referred immediately to the DSL and managed in accordance with safeguarding guidance.

5. Safeguarding and Reporting

Does this incident involve a potential safeguarding concern?

☐ Yes ☐ No ☐ To be determined by DSL

DSL/Deputy DSL informed: _____

Date and time informed: _____

External agencies contacted, where applicable:

- ☐ Children's Social Care
- ☐ Police
- ☐ LADO
- ☐ Other: _____
- ☐ Not applicable

Details of referrals or advice received:

6. Senior Team / DSL Review

Incident reviewed by: _____

Date of review: _____

Outcome / findings:

Further action required:

- ☐ Safeguarding follow-up
- ☐ Pupil support or education
- ☐ Parental meeting or communication
- ☐ Behaviour Policy procedures
- ☐ Staff conduct or disciplinary procedures
- ☐ Technical investigation or security action
- ☐ Filtering or monitoring review
- ☐ Policy or training review
- ☐ No further action
- ☐ Other: _____

Actions agreed, responsible person and timescale:

Rationale for decisions made:

7. Follow-Up and Closure

Follow-up completed:

Date completed: _____

Any further monitoring or review required?

☐ Yes ☐ No

Details:

Incident closed by: _____

Position: _____

Signature: _____

Date: _____

Record Keeping

This form must be stored securely in accordance with the Trust's data protection and records retention procedures. Where the incident involves safeguarding, the relevant information must also be recorded in the Trust's approved safeguarding system.

Access must be restricted to authorised personnel.

Appendix 8:**Parental permission form for image consent**

Permission For Photo and Video use at Dolphin School Parental Consent Form		
Do you give permission for the following:		
A. "External". Your child's photo/video to appear in an advert, in the school prospectus, in a magazine/newspaper, or on Social Media pages, in a promotional film or on the Dolphin's website? No child is ever identified by their full name.	Yes	No
B. "Internal". Your child to be included in photos such as class photos and cast photos, some of which appear on the coded section of the website and on the boards around school, as well as the printed school yearbook? (Please note that your child would have to be removed from a class or cast photo if permission is withheld.)	Yes	No
Signature:	Date:	