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:	April 2025
Next review:	January 2026

Introduction

Learning about technology is an increasingly essential life skill that all children should be aware of, understand, and be enabled to use effectively and safely.

This policy outlines principles of best practice regarding the use of IT in Dolphin School and Noah's Ark Nurseries. Online safety (e-safety) is recognised as both a statutory requirement and a standard embedded in our safeguarding principles and School ethos. It is defined not only by policy, but also by leadership, infrastructure, education, training, risk assessment, monitoring, and review.

This policy aligns with *Keeping children safe in education 2025* (KCSIE 2025), the Independent School Standards, the DfE's Filtering and Monitoring Standards (2023, updated 2024), and the DfE guidance on mobile phones in schools (2024). The Designated Safeguarding Lead (DSL) has lead responsibility for online safety, including oversight of filtering and monitoring. Governors/proprietors receive regular reports and ensure compliance with statutory requirements.

Dolphin School and Noah's Ark Nurseries expect all of their electronic and computer facilities to be used in an effective and professional manner and encourage all staff to develop the skills necessary to do so. These facilities are provided by the School and Nurseries at their own expense. They are to be used exclusively for designated purposes, to assist staff in carrying out their duties effectively and for the educational purposes of its pupils. It is the responsibility of each member of staff to ensure that this technology is issued and used for its proper purpose and in a manner that does not compromise the reputation of the School, Nurseries, or their staff in any way.

This policy applies at all times to all staff, including employees, contractors (self employed), casual, agency and volunteers who have access to the School IT systems.

All users are required to adhere to the conditions laid down in this policy. Any breach of these conditions may lead to immediate withdrawal of the user's access and investigation of the user's use of services. Any breach of these conditions will be considered a disciplinary matter and could result in criminal prosecution.

Contents

Linked Policies

This policy is linked to the following mandatory documents:
Safeguarding & Child Protection Policy, Health & Safety Policy, Staff Mobile Phone and Smart Device Use Policy, Behaviour Policy, Anti-bullying Policy

1. **Conditions of use**

Dolphin School and Noah's Ark Nurseries expect their staff to use IT in order to enhance learning within the curriculum, to acquire new skills; to provide guidance and instruction to pupils in the use of such resources. All pupil use of the internet will be within a lesson, for educational purposes, and under the supervision of a teacher. All computer systems will be regularly monitored to ensure that they are being used in a responsible and appropriate manner.

IT presents a form of communication that is permanent, traceable and accessible. All users must appreciate that, fundamentally, the main risks are not related to a piece of equipment, but to the behaviours of the individuals using it. The School email accounts must be the accounts used for all school business.

Under no circumstances, unless explicit permission has been given for a specified purpose, are staff permitted to contact pupils, parents or conduct school business using personal email addresses.

Personal responsibility

Access to online resources is a privilege, not a right. Users are personally responsible for their behaviour and communications. Staff and pupils are expected to use the resources for the purposes intended. Users are to take due care with the physical security of all hardware. Users will accept personal responsibility for reporting any misuse of the network to the Headteacher of Dolphin School and Noah's Ark Nurseries.

Acceptable use

Users are expected to utilise all IT resources and equipment in a responsible manner. Standards of acceptable use outlined in this section must be deemed the minimum baseline requirement. They provide guidelines and underlying principles. These standards are reiterated in the Acceptable Use Agreements which are signed by all staff users, pupils and parents, and can be found in the appendices to this policy. During exceptional circumstances, such as a pandemic, pupils will sign the Acceptable Use Agreement in school and the document is shared with parents.

Network etiquette and privacy

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

- Always log on with your own user ID and password. Do not share this information with other users. Log off the device after you have finished.
- Do not reveal your password to anyone. If you think someone knows your password, then contact a member of the Senior Team.
- Users finding a machine 'logged on' under another user's username should not use the computer under the other person's logging in details and should 'log off' the machine whether they intend to use it or not.
- Be polite online – never send or encourage others to send abusive messages
- Always use appropriate language online – users should remember that they are representatives of the School or Nurseries on a global communications system. Illegal activities of any kind are strictly forbidden.

- Keep email messages relevant and to the point. Ensure that an appropriate Subject Title is given.
- Be aware that the content of any email should be appropriate to communicate comfortably in person.
- Do not use language that could incite hatred against any ethnic, religious or other minority or protected characterising group; that may be considered extremist or offensive; that might be seen to promote radicalisation.
- Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users' files or folders.
- Be aware that highly confidential information (staff/pupil name and contact details, medical information, SEN register) must not be sent to email addresses outside of the school's domain.
- Electronic mail is not guaranteed to be private. Messages relating to, or in support of illegal activities, will be reported to the authorities. Do not send anonymous messages.
- Disruptions – do not use the network in any way that would disrupt use of the network by others.
- Do not attempt to visit websites that might be considered inappropriate. Such sites include those relating to illegal activity. All online activity is traceable on the School and Nursery network even after the individual computer used for access has been switched off. Downloading illegal material is an offence and the police or other authorities may be called to investigate such misuse.
- Pupils will not be allowed access to any computer without the supervision of a teacher. Staff or students discovering inappropriate use of the school network or a suspected breach of security must report it to the Deputy Heads immediately.
- It is the responsibility of the user (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this policy document, and to ensure that unacceptable use of the internet does not occur.

Unacceptable use

Examples of unacceptable use include, but are not limited to, the following:

- Accessing or creating, transmitting, displaying or publishing any material (for example images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety.
- Accessing or creating, transmitting or publishing any defamatory or extremist material.
- Receiving, sending or publishing material that violates copyright law.
- Receiving, sending or publishing material that violates the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018, or breaching the security these laws require for personal data.
- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.
- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.
- Deliberate interference with the School's IT filters; deliberate encryption or password protection of personal or illicit data on the School's domain.

Additional guidelines

- Users must comply with the acceptable use policy of any other networks that they access. Users must not download software or apps without prior approval from a member of the Senior Team.
- Subscriptions to new groups, mailing lists or other sites are only permitted when the subscription is for a work related purpose and then approved by the Senior Team.
- Emails leave a retrievable record and can be recovered; therefore staff are reminded to exercise caution when writing and sending emails.
- Staff sending emails to organisations or persons external to the School or Nurseries, are expected to adhere to the rules of acceptable use listed above. It is advisable to copy the Headteacher or appropriate senior member of staff into all external email correspondence.

2. **E-Safety Principles and Training**

The term e-safety encompasses the safe use of all forms of information and mobile communication technologies. The aim is to provide reasonable protection to all users from potential and known risk. For principles of e-safety to be effective, online procedures must be clear, agreed and respected.

This policy aims to increase awareness and understanding of online safety, to outline why certain procedures must be followed and to empower users to recognise, avoid and report dangers before they have an opportunity to escalate.

IT encompasses a wide range of media applications and connecting methods which are continually evolving and advancing. These include:

- Computers and laptops – access to fixed and mobile internet and apps email, skype, facetime, Snapchat, Instagram, chat-rooms, blogs, social media sites, podcasts, instant messaging, twitter etc.
- Wireless and broadband access
- Mobile/smart phones and devices with online access, Bluetooth, cameras etc
- Gaming – online and consoles
- Video broadcasting and music downloading
- Digital cameras

Promoting the safe use of online technologies both within the School and Nursery setting, as well as the home environment, are of the highest priority. We aim to provide an environment where children learn how to moderate their own behaviours and response to IT wisely, but are also enabled to recognise and respond safely to inappropriate behaviour in other users.

E-safety remains the responsibility of the Head, Senior Team, and Governors to ensure that policy and practices are shaped by our ethos, proactively informed by national and local guidelines, and compliant with ISA recommendations.

E-Safety Training

- All staff are reminded of the importance of e-safety.
- All staff members are required to sign the Acceptable Use Agreement for IT (see appendices to this Policy).
- Through Key Stage meetings and staff meetings, staff are reminded of their safeguarding responsibilities relating to e-safety, conditions of use of IT, including the procedure to follow in the event of misuse (see appendices).

- Staff are encouraged to incorporate e-safety activities to raise awareness within their curriculum areas.
- All new members of staff receive this policy and sign the Acceptable Use Agreement as part of their induction.
- An evening information session is given annually to parents to raise awareness of e-safety issues and to encourage healthy partnership with School and Nurseries staff. This may vary in format during exceptional circumstances, such as a pandemic.
- Staff are aware of the UKCIS advice regarding handling devices/images (especially when related to sharing nude and semi nude photos), when to inform police/CEOP, recording, parental contact.

E-Safety in the Curriculum

Principles of e-safety are embedded in all curriculum areas where IT is used to deliver or enhance education.

Across the Upper (KS2) and Lower (KS1) School, with a greater focus on children in the Upper School, all pupils are made aware of data protection issues, copyright and the appropriate attitude to intellectual property. Class teaching time and Relationship Time are used to raise awareness of, and vigilance to, cyber-bullying, and to enable children to respond promptly, safely and appropriately. The curriculum covers content, contact, conduct, commerce risks using UKCIS Education for a Connected World

Through cross-curricular models of teaching, all pupils are equipped to evaluate online material critically, to employ effective online search strategies, and to assess the merits of different online sources. The IT curriculum is regularly reviewed in order to keep abreast of current e-safety issues.

3. **Professional Behaviour**

Staff must ensure that their own online activity, both in school and outside of school, does not bring the school or their profession into disrepute. They must not talk about their professional role within the school when using social media.

Staff must make sure that their privacy settings on personal social network sites are set appropriately so that their own personal information is not available to the public. Staff must be aware that their reputation could be harmed by what others share online, such as tagging. Staff are encouraged to ensure that their friends and family contacts appreciate their professional responsibilities. Staff are advised to check their online presence regularly by entering their name into a search engine to see what is visible.

Staff are not to become a friend of a pupil (past or present) on a social networking site and are to reject requests and inform a member of the Senior Team.

It is wholly accepted that staff will use online and digital technologies in their personal and social lives. Neither the School nor the Nurseries seek to prevent any member of staff from accessing online technologies. However, we do ask them to understand that they are in a position of trust and that their actions outside of the professional environment could be misinterpreted by others, and to be conscious of this when sharing information publicly with others.

4. **Network Services and Security**

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at the user's own risk.

Network security

Users are expected to inform a member of the Senior Team immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must log in with their own user ID and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network. The procedure to follow, in the event of discovering misuse, is detailed in the appendices.

Staff are required to ensure that all school accounts are protected with strong passwords. Passwords should never be disclosed and if they are suspected to have been compromised, they must be changed immediately.

Staff must always ensure that their computer is locked if left unattended.

Other staff members or pupils are not permitted to use a device if it has been logged on by another individual.

Staff must never share a file containing personal information with another student and never use School external storage devices to store personal data.

Staff must never download personal data from the cloud to work with on a personal computer. Files should be accessed and modified on the Cloud or School network.

Physical security

Staff are expected to ensure that portable IT equipment such as laptops are placed in the safest available unit, for example the desk drawer of a secure cupboard. Staff are permitted to take laptops and Chromebooks home but the following conditions apply:

- Laptops and Chromebooks must be in school every day.
- The terms of this policy apply to the use of school computers on or off site.
- Laptops and Chromebooks must never be left in parked vehicles.
- Laptops and Chromebooks must never be left un-attended in a public place.
- Chromebooks must be signed in and out from the Lock n Charge storage unit.
- Confidential information about children (including children's names) must be guarded from public view at all times.
- Computer viruses can be sent by email or through memory sticks, causing damage to the school's systems. External files must be checked first before use on the school's network.
- If you suspect a virus, notify the Deputy Heads and the Dolphin School IT Technician.

Willful damage

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

5. Filtering and Monitoring

The School Reserves the right to monitor, intercept and read any internal or external email for the purposes of monitoring and record keeping to establish facts, to establish compliance with procedures, to prevent or detect crime, to investigate or detect the unauthorised use of

the School's computer system to ascertain compliance with the School's practices and procedures. The School may also monitor, intercept and read communications to check whether these are relevant to the School.
The School may carry out random spot checks on the email system in order to protect the security of its systems or investigate suspected wrongful acts.
The School may monitor websites visited and social media posts to check compliance with this Policy and the Acceptable Use Agreement.
The school has several layers of security built into their IT, including filters and an inappropriate use of internet alert system (Senso & Forticloud).

Dolphin School provides a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It's important that the right people are working together and using their professional expertise to make informed decisions.

Any concerns relating to extremist or radicalising material online will be managed in line with the School's Prevent Duty responsibilities and Safeguarding & Child Protection Policy. The DSL will liaise with external agencies as required, including the Local Authority Prevent Team and/or Police.

The following staff are responsible for the filtering and monitoring of network traffic, access to websites and online behaviour within the Dolphin School network:

Adam Woodcraft, DSL – Receives emails when the filtering rules trigger mis-use or a violation of the filtering. The DSL will perform a check with the IT contractor/manager regularly to ensure the filtering is active and working under a safe environment. This is logged in the safeguarding review.

Lucy Price, Headteacher – Receives monthly digests of online behaviour and traffic from the filtering system in order to monitor usage.

Staff – Staff are regularly reminded in briefings, staff meetings and annual InSET sessions that they have a duty to monitor pupils' usage of the internet and school network whilst teaching and supervising children. Active monitoring and responding to the needs of the children when using technology is required. Staff must report any concerns about inappropriate behaviour to a member of the Senior Team and/or log the incident in Engage.

Mike Sutcliffe – IT contractor will monitor the filtering software to ensure it is up to date and effective.

Johnny Savile - Safeguarding Governor with responsibility for liaising with the DSL on filtering and monitoring, incidents, training, review outcomes.

In line with the DfE Filtering and Monitoring Standards, the Headteacher is the Senior Responsible Owner (SRO) for filtering and monitoring. An annual written review of filtering and monitoring is undertaken by the DSL, IT contractor and Headteacher, and formally reported to governors.

An annual online safety risk assessment is completed, mapped to the 4Cs of online risk (Content, Contact, Conduct, Commerce).

Filtering and monitoring apply to all devices using the school's networks, including personal devices (staff and visitors). Pupils are prohibited from circumventing these protections (e.g. hotspot tethering or VPN use). Remote filtering is enabled on school devices used off-site.

6. Use of Personal Mobile Devices

Staff must ensure that their own mobile devices (tablets and phones) are always protected by a passcode to prevent unauthorised access.
Dolphin School provides staff with a mobile phone for emergency use when off-site, during break and school trips. The School and Nurseries also make available mobile devices for day trips and outings, and only these devices are to be used in an appropriate manner.

The sending of inappropriate text messages between any members of the school community is not allowed, regardless of whether a school or personal phone is used.

In line with DfE guidance (2024), pupils must not use mobile phones during the school day. Where phones are brought into school, they must be handed in/stored securely as set out in the Behaviour Policy. Searching, screening and confiscation will follow DfE statutory guidance (July 2022).

Please refer also to appendices and to the Staff Mobile Phone and Smart Device Use Policy.

7. Media publications and Safe Use of Images

Digital images are easily captured, stored, reproduced and published. The same basic principles for e-safety apply.

Staff are forbidden to take images of pupils and/or staff with their own device.

School cameras or Ipads must always be used, and then only for strictly designated purposes. On a child's entry to the School or Nurseries, all Parents/Carers are asked to give signed permission for photographs of their child to be used for specified purposes e.g. display material in communal areas of the School or Nurseries, for use in the prospectus, in school matches and drama productions etc.

This consent form is considered valid for the entire duration of the child's attendance. Parents/Carers can withdraw permission, in writing, at any time. The names of pupils will not be published alongside their image under any circumstances.

There is a record on the school management system of all the children for whom permission regarding photography has been granted by Parents/Carers. It is the responsibility of all staff to check this list before taking photographs. In particular, class teachers must aim to be familiar with information regarding permission for children in their class.

If the children's work is to appear in a publication with external distribution (i.e. not a school publication such as a school yearbook which is offered internally to staff and parents), parents will be given the opportunity to withdraw their child.

Images of children for whom permission has been given, are stored on school computers. Pupils and staff are not permitted to use personal portable media e.g. USB sticks, to store images without permission from the Senior Team. Rights of access to this material are restricted to teaching staff and pupils, within the appropriate context of school activity.

Webcams are not to be used to record either pupils or staff. They can be used for specific learning objectives e.g. monitoring incubated hens' eggs, or an agreed online video call. Misuse of a school webcam by any member of the school community will result in disciplinary action.

The school does not publish pupils' full names alongside images. Where images are used for promotional or online purposes, the lawful basis is parental consent; where images are used internally (e.g. class displays), the lawful basis may be legitimate interests, with an opt-out available

The parental permission letter for image consent, and relevant forms that cover use, storage and reproduction of images, can be found in the Appendices.

8. Equal Opportunities

Dolphin School and Noah's Ark Nurseries endeavour to create a consistent message to parents for all pupils. Staff are aware that some pupils may require additional support in the use of IT, including prompts and further explanation to reinforce existing knowledge and understanding of e-safety priorities. All online activities are planned and proactively managed for these children.

Parents and Carers are encouraged to contribute to our e-safety practice by reporting unsuitable sites. Parent/Carer(s) are asked to read through with their child/children and sign Acceptable Use Agreements (see appendix) on their behalf of their child, for every academic year. During extenuating circumstances, such as a pandemic, physical signing by parents is not required. The school disseminates any information to parents relating to e-safety in our weekly newsletter.

9. Breaches of this policy

The School considers this policy to be extremely important. If an employee is found to be in breach of the policy, they will be disciplined in accordance with the Grievance, Disciplinary and Capability Policy and may be dismissed.

In certain circumstances, breach of this policy may be considered gross misconduct, resulting in immediate termination of employment or contract without notice or payment in lieu of notice.

Please refer to appendices for the procedure to follow in the event of misuse of IT. Complaints relating to e-safety will be addressed according to the School and Nurseries' Complaints Policy.

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

Appendix	Item
Appendix 1	Acceptable Use Agreement for Staff
Appendix 2	Acceptable Use Agreement for PE, Dance and Music Staff
Appendix 3	Acceptable Use Agreement for Upper School Pupils
Appendix 4	Acceptable Use Agreement for Lower School Pupils
Appendix 5	Particular e-safety considerations in the EYFS setting
Appendix 6	Procedure to follow in the event of IT misuse by a staff member
Appendix 7	Procedure to follow in the event of IT misuse by a pupil
Appendix 8	Incident form to report IT misuse
Appendix 9	Parental permission form for image consent
Appendix 10	Social Media guidelines
Appendix 11	Use of AI in School

Appendix 1:

Dolphin School Acceptable Use Agreement for Staff

To ensure that staff are fully aware of their responsibilities with respect to IT use (including email, internet and network resources, Apps, software, equipment and systems), they are asked to sign this Acceptable Use Agreement.

- I understand that this agreement is in line with the Dolphin School & Noah's Ark Nurseries E-Safety Policy and will ensure that I have read and understood the latest version.
- I understand that the Dolphin School Google environment is the property of the school and agree that my use must be compatible with my professional role.
- I agree and accept that any device loaned to me by the school is provided solely to support my professional responsibilities.
- I will not allow unauthorised individuals to access the school's Google platform or other school systems.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not confused with my professional role.
- I understand that the school IT systems may not be used for private purposes.
- I will only use the approved, secure school email system(s) for any school business (currently Outlook and Google Mail), including communication with pupils, colleagues and parents/carers.
- I will respect IT system security and understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I understand that personal mobile phones may only be used during out of school hours and during break times and where pupils are not present.
- I understand that personal mobile phones must not be used in EYFS classrooms, outdoor play areas, or when supervising children.and that they must be kept in locked boxes, the staffroom, or another designated secure area during contact time with EYFS children.
- I will not take photographs with any other camera other than the school cameras. This includes mobile phone cameras, which will not be used for taking photographs of any pupils or families within the setting. I will not store any photographs of pupils or families outside of the secure set up on the school's Google Drive.
- If an allegation has been made concerning the safety of a staff member or pupil, I understand and agree that the school may monitor my network, internet and mobile technology use.
- I will not download/install any software or applications without permission from a member of the Google Admin team or a member of the Senior Team.
- I understand that I am not allowed to download applications which require payment without permission.
- I will not disclose any password or login details to anyone other than, where appropriate, the Google Admin team.

- I will take all reasonable precautions to secure data or equipment taken off the School premises.
- I will not browse, download or send material that could be considered offensive to colleagues, parents or pupils.
- I will report any accidental access, receipt of inappropriate materials, or filtering breach to the Computing Coordinator or to a member of the Senior Team.
- I will report any safeguarding incidents of concern to the Designated Safeguarding Lead.
- I will ensure that my electronic communications with others in the Dolphin School community are compatible with my professional role and cannot be misinterpreted.
- I will promote e-safety with the pupils, in order to develop a responsible attitude towards using technology e.g. in the use of passwords.
- I will respect copyright and intellectual property rights.

The School may exercise its right to monitor the use of the School's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the School's computer system may be taking place, or if the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Updated: April 2025

Staff Name ……………………………………………

Staff Signature ……………………………………..…

Date : ………………………………………………

Senior Team Signature:……………………………

Appendix 2:

Dolphin School Acceptable Use Agreement
for PE, Dance & Music Staff

To ensure that staff are fully aware of their responsibilities with respect to IT use (including email, internet and network resources, Apps, software, equipment and systems), they are asked to sign this Acceptable Use Agreement.

- I understand that this agreement is in line with the Dolphin School E-Safety Policy and will ensure that I have read and understood the latest version.
- I understand that the Dolphin School Google environment is the property of the school and agree that my use must be compatible with my professional role.
- I agree and accept that any device loaned to me by the school is provided solely to support my professional responsibilities.
- I will not allow unauthorised individuals to access the school's Google platform or other school systems.
- I will not engage in any online activity that may compromise my professional responsibilities or bring the school into disrepute.
- I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not confused with my professional role.
- I understand that the school IT systems may not be used for private purposes.
- I will only use the approved, secure school email system(s) for any school business (currently Outlook and Google Mail), including communication with pupils, colleagues and parents/carers.
- I will respect IT system security and understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I understand that personal mobile phones may only be used out of school hours and during break times and where pupils are not present. During educational visits and school trips I may use my personal mobile phone, as an exception, for school related business.
- As a Physical Education staff member, I understand that I may have my personal mobile phone on my person. However, I acknowledge that, where possible, my phone will remain out of sight of children and may only be used for urgent PE communications, such as contacting other schools in the event of a match cancellation or clarifying logistics when travelling to and from facilities.
- As a music/dance teacher, I acknowledge that I can use my mobile phone to play digital music during class, assembly or clubs.
- I will not use my mobile phone for personal use where pupils are present.
- I will not take photographs with any other camera other than the school cameras. This includes mobile phone cameras, which will not be used for taking photographs of any pupils or families within the setting. I will not store any photographs of pupils or families outside of the secure set up on the school's Google Drive.
- If an allegation has been made concerning the safety of a staff member or pupil, I understand and agree that the school may monitor my network, internet and mobile technology use.
- I will not download/install any software or applications without permission from a member of the Google Admin team.

- I understand that I am not allowed to download applications which require payment without permission.
- I will not disclose any password or login details to anyone other than, where appropriate, the Google Admin team.
- I will take all reasonable precautions to secure data or equipment taken off the School premises.
- I will not browse, download or send material that could be considered offensive to colleagues, parents or pupils.
- I will report any accidental access, receipt of inappropriate materials, or filtering breach to the Computing Coordinator or to a member of the Senior Team.
- I will report any safeguarding incidents of concern to the Designated Safeguarding Lead.
- I will ensure that my electronic communications with others in the Dolphin School community are compatible with my professional role and cannot be misinterpreted.
- I will promote e-safety with the pupils, in order to develop a responsible attitude towards using technology e.g. in the use of passwords.
- I will respect copyright and intellectual property rights.

The School may exercise its right to monitor the use of the School's computer systems. This includes access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the School's computer system may be taking place, or if the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Updated: April 2025

Staff Name ……………………………………………

Staff Signature ………………………………..…

Date : ……………………………………………….

Senior Team Signature:……………………………

Appendix 3

Dolphin School Acceptable Use Agreement for Upper School Pupils (Y3-6)

These rules will keep everyone safe and help us to be fair, kind and respectful to others.

- I will only use my Chromebook for my school work.
- I will keep my password secret. Only my teachers can know.
- I will not try to find out or use other people's passwords.
- I will not bring USB sticks or memory cards into school.
- I will only search on Google when my teacher tells me to do so.
- I will only use my emails when my teacher tells me to do so. These emails will only be to pupils and teachers in Dolphin school.
- I will never give out my Google Mail address to anyone outside of Dolphin School.
- I will only send messages which are polite and sensible.
- I will not send my home address or phone number by email.
- I will not send a photograph or video to anyone by email.
- If I see anything that makes me unhappy, I will tell a teacher straight away.

Additional rules for Remote Learning

- I will only use technology for school work in the way that my teacher tells me.
- I will only use technology when an adult from my house has given me permission to use it.
- I will make sure that all my messages to other people, including teachers and my classmates, are sensible and responsible.
- I will not use video content from my teacher outside the Google Classroom.

Additional rules for face-to-face video conferencing (such as Google Meet):

- I will be punctual, at the allotted time, for my video conferencing session.
- I will be patient and respectful of my teacher and classmates.
- I will remain muted/quiet until the class teacher invites me to speak.
- I will raise my hand as I would in school in order to speak.
- I will be fully dressed in appropriate clothes, ie. not in pjs or swimwear.
- I will be sitting in a chair, preferably at a table/desk- not lounging in bed or on a sofa.

- I will video conference from an environment that is safe, quiet and free from distractions (outside is not ideal due to sun glare and atmospheric noise).
- If using an ipad or tablet, I will ensure that it is on a sturdy surface or use a tripod/stand.
- I will not not use the chat feature unless asked to by the teacher.
- I will not record or take photos of my classmates or teachers during face-to-face sessions.

My teacher has explained these rules to me and I understand them. I will obey these rules at all times. If I do not follow these rules, I may not be allowed to use the Chromebooks for a while.

Pupil Name (printed) ……………………………………. Year Group ……………....

Pupil Signature ………………………………………… . Date ……………………..

Class Teacher Signature……………………………….... Date ……………………

updated April 2025

Appendix 4:

Dolphin School Acceptable Use Agreement for Lower School Pupils (Y1-2)

These rules will keep everyone safe and help us to be fair, kind and respectful to others.

- I will only use my Chromebook for my school work.
- I will keep my password secret. Only my teachers can know.
- I will not try to find out or use other people's passwords.
- I will not bring USB sticks or memory cards into school.
- I will only search on Google when my teacher tells me to do so.
- I will only use my emails when my teacher tells me to do so. These emails will only be to pupils and teachers in Dolphin school.
- I will never give out my Google Mail address to anyone outside of Dolphin School.
- I will only send messages which are polite and sensible.
- I will not send my home address or phone number by email.
- I will not send a photograph or video to anyone by email.
- If I see anything that makes me unhappy, I will tell a teacher straight away.

Additional rules for Remote Learning

- I will only use technology for school work in the way that my teacher tells me.
- I will only use technology when an adult from my house has given me permission to use it.
- I will make sure that all my messages to other people, including teachers and my classmates, are sensible and responsible.
- I will not use video content from my teacher outside the Google Classroom.

Additional rules for face-to-face video conferencing (such as Google Meet):

- I will be punctual, at the allotted time, for my video conferencing session.
- I will be patient and respectful of my teacher and classmates.
- I will remain muted/quiet until the class teacher invites me to speak.
- I will raise my hand as I would in school in order to speak.
- I will be fully dressed in appropriate clothes, ie. not in pjs or swimwear.
- I will be sitting in a chair, preferably at a table/desk- not lounging in bed or on a sofa.
- I will video conference from an environment that is safe, quiet and free from distractions (outside is not ideal due to sun glare and atmospheric noise).

- If using an ipad or tablet, I will ensure that it is on a sturdy surface or use a tripod/stand.
- I will not not use the chat feature unless asked to by the teacher.
- I will not record or take photos of my classmates or teachers during face-to-face sessions.

My teacher has explained these rules to me and I understand them. I will obey these rules at all times. If I do not follow these rules, I may not be allowed to use the Chromebooks for a while.

Pupil Name (printed) …………………………………… Year Group ……………....

Pupil Signature ……………………………………… Date ……………………..

Class Teacher Signature………………………………… Date …………………….

updated April 2025

Appendix 5:

Particular Considerations for E-Safety in the EYFS setting

This appendix outlines particular IT issues for Reception classes at Dolphin School and the two Noah's Ark Nurseries.

The influence and value of IT is increasingly relevant to Early Years Foundation Stage. The ethos of the School and Nurseries is firmly embedded in guidelines for IT use and proactive awareness of e-safety. Particularly in this younger age group, the indirect, as well as the direct, impact of IT on learning and development should be carefully considered.

By the end of Foundation Stage, most children will be able to identify uses of everyday technology and demonstrate use of IT to enhance their learning.

Early years teachers at our School and Nurseries employ a wide range of IT resources to manage their professional roles. This includes using online systems to track progress and record Individual Learning Plans, and for effective communication and administrative purposes.

Effective online safety practice will enable young children to use technology safely, whether at home, in the early years setting or within the social environment. It will empower them to use their acquired skills and knowledge to keep themselves safe, without limiting opportunities for exploration, creativity and innovation.

Staff must not use personal mobile phones in EYFS classrooms, outdoor play areas, or when 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 only use personal phones in the staffroom or office during breaks, and never in areas where children are present.

Mobile phones must not be used to take photographs, videos, or recordings of children under any circumstances. All images must be taken on school devices in line with safeguarding and GDPR procedures.

In the event of an emergency, staff must use the school landline or an agreed school mobile phone. If personal phones are required (e.g. during a trip), this must be authorised by the Headteacher, and phones should only be used for emergency contact and not for personal reasons.

Visitors, volunteers, and contractors are also expected to follow this policy: mobile phones must not be used in EYFS areas and never for taking photos or videos of children.

Named designated E-Safety lead at each site:

Noah's Ark Nursery, Dolphin : Mr Adam Woodcraft

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

Appendix 6:

Procedure to follow in the event of IT misuse by a member of Staff

Accidental access to inappropriate material must be reported immediately to the Designated Safeguarding Lead:

Dolphin School: Mr Adam Woodcraft

In their absence, the incident should be reported to a Deputy DSL:

Dolphin School & Noah's Ark Nursery, Dolphin: Mrs Lucy Price, Mr Jeff Schmidt, Mrs Victoria Githae

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

All Staff members sign an Acceptable Use Agreement which informs them of the appropriate standard of behaviour expected to ensure online safety for themselves and others.

The Acceptable Use Agreement also informs Staff of behaviours which are deemed unacceptable.

In understanding and signing Acceptable Use Agreements, Staff are made aware of the potential risks associated with IT misuse and the sanctions which will be applied, where necessary.

Deliberate access to inappropriate material, wilful contravention of the rules set out in this policy, by any user, will constitute a disciplinary matter.

All incidents of this nature will be logged and investigated by the Senior Team.

An investigation by the Head for serious infringement of IT use may require immediate suspension of the user from Dolphin School and Noah's Ark Nurseries.

In certain circumstances, breach of this policy may be considered gross misconduct resulting in immediate termination of employment or contract without notice or payment in lieu of notice.

If an allegation of a serious offence is substantiated, the results of the investigation may lead to dismissal and referral to the Police.

Appendix 7:

Procedure to follow in the event of IT misuse by a Pupil

Accidental access to inappropriate material must be reported immediately to the Designated Safeguarding Lead:

Dolphin School: Mr Adam Woodcraft

In their absence, the incident should be reported to a Deputy DSL:

Dolphin School & Noah's Ark Nursery, Dolphin: Mrs Lucy Price, Mr Jeff Schmidt, Mrs Victoria Githae

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

All children in Y1-6 sign an Acceptable Use Agreement which informs them of the appropriate standard of behaviour expected to ensure online safety for themselves and other users.

The Acceptable Use Agreement also informs children of behaviours which are deemed unacceptable. This encourages them to take some degree of responsibility for their own actions.

In understanding and signing Acceptable Use Agreements, children become aware of the potential risks associated with IT misuse and the sanctions which will be applied, where necessary.

Step 1: Deliberate access to inappropriate material, or any wilful contravention of the Acceptable Use Agreement, by any user, will always be taken seriously.

In the first instance, the child's parent/carer will be informed, outlining the issue. The child may be temporarily suspended from use of IT equipment.

Step 2: If there are further incidents of misuse, the child will be suspended from using the internet or other relevant technology for an increased period of time.
The parent or carer will be invited to discuss the incident in more detail with the Headteacher or member of the Senior Team, and the most appropriate course of action will be agreed.

Step 3: The sanctions for misuse can be escalated at any stage, should it be considered necessary. In the event that misuse is deemed to be of a sufficiently serious nature, steps 1 and 2 can be omitted.
Should a child or young person be considered to be at risk of significant harm, the Dolphin School Safeguarding & Child Protection Policy will also be applied.
Allegations of serious misuse will be reported to the most appropriate agency e.g. the Police or Wandsworth Council Social Services.

All incidents of this nature will be logged and investigated by the Senior Team.

Appendix 8

Incident Form for reporting IT Misuse

To be completed as thoroughly as possible by the person who identified the incident.

Name of staff member reporting:	
Date of incident:	
Time(s) of incident:	
If repeated, duration of misuse: **(e.g. One off, a week, 2 months etc.)**	
Place of incident:	
How was the incident identified? e.g. by member of staff, informed by third party etc.	

Who was involved in the incident of IT misuse and how do you know this? **Is there any evidence to suggest that false names/details have been given?** **Give full details of real names and email addresses etc where known.**
Description of the online safety incident, including detail of specific services or websites used (e.g. chat room, instant messenger), email addresses, usernames etc.

Why do you have concerns about this incident?

Is anyone else aware or involved in this incident?

Name of Staff member (completing form):

Signature:

Position:

Date:

Has the information been recorded and secured?	**Yes/No**
Has the computer or hardware been secured?	**Yes/No**
If yes, by whom?	
What actions were taken, by whom and why? **Give detail of agencies informed and contact person within those agencies.**	
Follow-up?	

Senior Team

Name:

Signature:

Date:

Appendix 9:

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:**	

Appendix 10:

Social Media guidelines

ETHOS

- Must reflect our identity (**relationships, nurturing, successful, joyful**)
- Primarily a marketing tool. *Key question: Is it appealing beyond our parents?*
- Showing who we are and what we do without becoming a newsfeed.
- Highlighting events to prospective parents (scholarship days, registration deadlines, open days, prospective parents mornings)
- Broad brushstrokes

CONTENT OF THE PAGE

- Hashtags (use staple hashtags on all posts)
- Love. Wisdom. Truth.
  #lovewisdomtruth #londonschools #educationmatters #learning #school #education #dolphinschoollondon #dolphinschool #christian #independentschool #claphamjunction #northcoteroad #nappyvalley #wandsworthcommon #wandsworth #swlondon
- Signature: **Love, Wisdom, Truth** under each post
- Copy always double checked by Senior Team
- 'No Comments' enabled

STYLE OF THE PAGE

- Filter (if needed, use warm and bright)
- Fonts- Palatino and Gill Sans MT
- Keep a rhythm of photos and quotes
- Aim to use brand colours where possible

Appendix 11:

Use of AI in School

Contents

Introduction

Dolphin School Trust's AI policy aims to harness the power of Artificial Intelligence (AI) to enhance educational experiences, support staff wellbeing through workload reduction, and promote an understanding and ethical use of AI among students and staff. A key focus is on safeguarding data privacy in compliance with GDPR. Our policy outlines clear guidelines for approval and accountability, ensuring responsible and effective integration of AI technologies in our educational framework. Through this policy, we are committed to balancing innovation with ethical responsibility, fostering an inclusive and advanced learning environment.

Objectives

Dolphin School Trust's AI policy is designed:

1. To enhance the educational experience through the integration of AI.
2. To support staff wellbeing through workload reduction using AI.
3. To promote an understanding and ethical use of AI among students and staff.
4. To protect the data privacy and rights of our school community in line with GDPR.

Enhancing educational experience through the integration of AI.

1 Student facing AI teaching applications

These are AI-powered tools that directly interact with students, offering personalised learning experiences. They include adaptive learning platforms, intelligent tutoring systems, language learning applications, and interactive educational games.

Examples include:

- **Adaptive Learning Platforms:** Customise content and difficulty based on student performance.
- **Intelligent Tutoring Systems:** Offer personalised guidance and feedback, simulating a one-on-one tutoring experience.
- **Interactive Educational Games:** Adapt challenges to match the student's learning curve.

Guidance at Dolphin School Trust in Adopting Student-Facing AI Tools

- **Understand the Tool:** Teachers and leadership must familiarise themselves with AI tool capabilities and integration methods.

- **Data Privacy:** Ensure compliance with data privacy laws (see below).
- **Supplement Teaching:** Use AI tools to enhance, not replace, traditional teaching.
- **Monitor and Evaluate:** Regularly assess the effectiveness of AI tools.
- **Professional Development:** Receive training in using AI tools effectively (see below)
- **Encourage Critical Thinking:** Promote critical evaluation of information provided by AI.
- **Equity and Accessibility:** Ensure AI tools are accessible to all students, including those with SEND and are used to enhance inclusion.

2 Planning and preparation AI applications

Teacher-facing AI tools are designed to aid educators in the creation, organisation, and optimisation of lesson plans and teaching resources. These tools leverage AI to analyse educational content, student data, and learning outcomes to suggest or generate tailored teaching strategies and materials.

Examples include:

- **AI-powered resource creation tools:** AI tools can be used to create lesson plans, or resources saving time (see more below) and personalising resources to particular needs of pupils or groups of pupils.
- **AI-driven Curriculum Development:** AI tools can suggest updates and improvements to the curriculum based on emerging educational trends, student performance data, and global best practices.
- **Personalised Content Recommendations:** AI systems can recommend educational content and activities tailored to the class's learning level, interests, and past performance.

Guidance at Dolphin School Trust in Adopting AI Tools for Planning

- **Explore and Understand:** Teachers should explore various AI tools to understand their features and how they can best be integrated into their lesson planning.They should request training if required (see below) to help develop their understanding.
- **Data-Informed Decisions:** Teachers should use AI tools to make informed decisions about lesson content and structure, while maintaining pedagogical autonomy.
- **Collaborative Planning:** AI tools can be used to facilitate collaboration among teachers, enabling the sharing of resources and best practices.
- **Continuous Learning:** Engage in ongoing professional development to stay updated with the latest AI tools and methodologies in education (see below)
- **Feedback and Adaptation:** Regularly gather feedback on the effectiveness of AI-aided lesson plans and adapt strategies accordingly.
- **Ethical Considerations:** Ensure that the use of AI respects student privacy and promotes equitable access to education. Staff must not enter special category data or pupil-identifiable data into generative AI tools without: (a) a documented lawful basis, (b) a completed Data Protection Impact Assessment (DPIA), and (c) a signed Data Processing Agreement with the provider.
- **Data compliance:** Ensure AI tools comply with relevant data regulations (See below)

3 Data analysis AI applications

These AI tools are designed to help teachers analyse various forms of educational data, including test scores, attendance records, and engagement metrics. By leveraging AI, educators can gain deeper insights into student performance, learning trends, and areas needing attention.

Examples include

- **Performance Analytics:** AI tools can analyse test scores and other performance indicators to identify trends, strengths, and areas for improvement in student learning.
- **Predictive Analytics**: These systems use historical data to predict future performance, helping educators to proactively address potential learning gaps and challenges.
- **Engagement Tracking:** AI can assess student engagement levels through analysis of class participation, assignment completion rates, and online learning interactions.
- **Customised Intervention Strategies:** Based on data analysis, AI can suggest targeted intervention strategies for individual students or groups, tailored to their specific needs.

Guidance at Dolphin School Trust in Adopting AI Tools for Data Analysis

- **Understanding Data:** Teachers should develop a foundational understanding of data analysis principles to interpret AI-generated insights effectively.
- **Ethical Use of Data:** Ensure that all data analysis adheres to ethical standards and respects student privacy and confidentiality.
- **Balancing AI and Human Judgment:** Use AI as a tool to supplement, not replace, professional judgement in educational decision-making.
- **Professional Development:** Engage in training to enhance skills in data analysis and the use of AI tools.
- **Collaborative Insights:** Share and discuss AI-generated insights with colleagues to foster a collaborative approach to student development.
- **Feedback Loop:** Establish a feedback loop to continuously refine and improve the use of AI tools based on real-world classroom experiences and outcomes.
- **Data compliance:** Ensure AI tools comply with relevant data regulations (See below)

Supporting staff wellbeing through workload reduction using AI.

Dolphin School Trust aims to leverage the power of AI to support teacher wellbeing by reducing workload. AI-powered tools such as TeachMateAI can achieve this. TeachMateAI, an AI-powered digital assistant for teachers, offers a range of tools designed to significantly reduce the workload of teachers, thereby enhancing the efficiency and effectiveness of their teaching practices.

Examples of TeachMateAI's tools include:

- **Automating Administrative Tasks:** TeachMateAI specialises in automating tasks. These include creating bespoke lesson plans, instant teacher presentations, and generating personalised student reports. This automation allows teachers to devote more time to direct student interaction and pedagogical planning.
- **Content Creation and Management:** Teachers often spend a significant amount of time creating educational content like model texts and comprehension texts. TeachMateAI assists in this process, generating high-quality content that can be used in classroom instruction.
- **Streamlining Lesson Planning:** The AI tool aids in lesson planning by providing templates and suggestions based on curriculum requirements and student data. This

feature enables teachers to develop comprehensive lesson plans more quickly and efficiently.

Professional responsibility

In the integration of AI tools to support teaching and reduce workload, it's crucial to emphasise the professional responsibility and oversight of teachers at Dolphin School Trust retain in managing and utilising these tools. While AI offers substantial benefits in terms of efficiency and personalization, the ultimate responsibility for the educational process remains with the teachers. A register of approved AI tools is maintained by the Senior Team. New tools require a formal proposal, DPIA, and senior approval before use. This section outlines key aspects of maintaining professional responsibility and oversight when using AI tools in education.

Understanding and Expertise

- **Continuous Learning:** Teachers should engage in ongoing professional development to understand the capabilities and, importantly, the limitations of AI tools. This knowledge enables them to effectively integrate AI outputs into their teaching strategies.
- **Critical Evaluation:** Educators must critically evaluate and interpret the data and suggestions provided by AI tools, using their professional judgement to make final decisions.

Ethical Use and Data Privacy

- **Adherence to Ethical Standards:** Teachers must ensure that the use of AI tools aligns with ethical standards in education, particularly regarding fairness, transparency, and inclusivity.
- **Data Privacy Compliance:** Educators are responsible for safeguarding student data. It's imperative to ensure that AI tools comply with data privacy laws and school policies (see below).

Oversight and Feedback

- **Monitoring AI Tools:** Regular monitoring of the AI tools is essential to ensure they function as intended and contribute positively to the learning process.
- **Feedback Loop:** Establish a system for providing feedback on the AI tools' performance, contributing to their continuous improvement.

Collaboration and Communication

- **Collaborative Approach:** Encourage collaboration among educators in using AI tools, promoting the sharing of experiences, insights, and best practices.
- **Communicating with Stakeholders:** Maintain open communication with students, parents, and administrators about the role and impact of AI tools in education, ensuring transparency and building trust - see below.

Promoting an understanding and ethical use of AI among students, staff and wider stakeholders.

Staff training

At Dolphin School Trust we believe comprehensive staff training is essential for the effective integration of AI in education. It equips educators with a thorough understanding of AI tools, allowing them to enhance teaching and learning experiences. Training also ensures adherence to ethical standards and data privacy, important when handling sensitive student information. An appropriate series of professional training will accompany the adoption of AI applications. Staff training on AI will form part of annual CPD, aligned with DfE AI in education guidance (2025). Governors will receive updates on the use and impact of AI within school.

Transparency with stakeholders: pupils, parents, governors

In implementing AI in education, transparency with stakeholders - pupils, parents, and governors - is crucial. Dolphin School Trust will communicate with our community where, how and why we are using AI. Pupils should understand how AI impacts their learning, while parents need to know how it enhances education and safeguards privacy. Governors require detailed updates on AI strategies, educational impacts, and ethical compliance.

Ensuring AI tools are appropriately data compliant

In adopting AI tools at Dolphin School Trust, it is imperative we ensure compliance with the General Data Protection Regulation (GDPR). GDPR compliance is crucial for protecting the privacy and personal data of students and staff, and for maintaining the integrity and trustworthiness of the educational institution. The following points outline key considerations in ensuring that AI tools are GDPR compliant:

- **Data Protection by Design:** Choose AI tools that are built with data protection as a core feature. This includes robust encryption, secure data storage, and minimal data collection in line with GDPR requirements.
- **Consent and Transparency:** Ensure that clear consent is obtained from students and staff for the collection and use of their data. Provide transparent information about what data is being collected, how it will be used, and who will have access to it.
- **Data Minimization:** Adopt AI tools that only collect and process the data necessary for the intended educational purpose. Unnecessary data collection must be avoided to minimise privacy risks.
- **Data Subject Rights:** The AI tools should facilitate the rights of data subjects, including the right to access, rectify, and erase their personal data, as well as the right to object to data processing and the right to data portability.
- **Data Processing Agreements:** Ensure that agreements with AI tool providers include clauses that require them to comply with GDPR. This includes provisions for data protection, processing limitations, and obligations in case of data breaches.
- **Regular Audits and Assessments:** Conduct regular audits of AI tools to ensure ongoing compliance with GDPR. This includes assessing the data protection impact, particularly when introducing new tools or making significant changes to existing ones.
- **Training and Awareness:** Provide training for staff and students (if appropriate) on GDPR compliance, focusing on their roles and responsibilities in protecting personal data when using AI tools.

- **Incident Response Plan:** Develop and maintain an incident response plan to address any data breaches or GDPR non-compliance issues promptly and effectively.

Approval and Accountability

Designated school leaders overseeing AI implementation

This policy operates in conjunction with the school's Data Protection Policy. All IT and AI systems are required to comply with UK GDPR and the Data Protection Act 2018. DPIAs are completed for any high-risk processing, including the adoption of new edtech and AI tools. Privacy notices for staff, pupils and parents explain how data is collected, used and monitored, including in relation to online safety and filtering.

To ensure a structured and responsible approach to AI implementation in the school, designated school leaders are assigned to oversee this integration. At Dolphin School Trust, this is the senior team. These leaders are responsible for guiding and supervising all aspects of AI adoption. Their roles include evaluating the educational value of proposed AI tools, ensuring compliance with legal and ethical standards, and aligning AI initiatives with the school's educational goals and policies.

These leaders facilitate cross-departmental collaboration (where appropriate in secondary settings), ensuring that the voices of educators, IT staff, and other stakeholders are considered in the decision-making process. Regular training and professional development are provided to these leaders to keep them updated on the latest AI advancements and best practices in educational technology.

Processes for sign off on the introduction of AI tools

The introduction of AI tools at Dolphin School Trust follows a formalised approval process to ensure accountability and alignment with the school's educational objectives. This process includes: a detailed proposal, including the purpose, benefits, costs, and potential risks associated with the AI tool. The aforementioned designated leaders overseeing AI implementation at Dolphin School Trust will approve or decline proposals.