E-Safety Policy

Introduction

E-Safety reflects the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole. E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones, worn or handheld devices and wireless technology. It highlights the need to educate children and parents about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable parents to take control of their children's online experiences. E-safety is important for all staff to understand so that they can keep children safe and support parents by implementing the e-safety policy and procedures.

Background

At Alamiyah we believe in the vast learning benefits that come from responsible use of online technologies at an appropriate time in a child's life. All staff use technology in their work to advance pupil learning. At the setting, pupils do not use screens, they are encouraged to use offline and screen free technology as far as possible to build their understanding of its mechanics which will prepare them for the use of technology when they are older. Parents are encouraged to provide a home environment and play which is screen free for their children and to use offline technologies. At Alamiyah we are aware of both the advantages and dangers of the use of technology and strive to support children, staff and families to use the internet safely.

Aims

At Alamiyah we will ensure the responsible usage of electronic devices for data storage, cameras, mobile phones, internet, email and social networking sites by management, staff, visitors and pupils. We take all steps to ensure that there are effective procedures in place to protect children from unacceptable use of Information Communication Technology. As a result, we aim to ensure that:

- pupils are protected from harmful or inappropriate online material

- parents and pupils are educated about e-safety including the benefits, risks and responsibilities of using online technology and electronic communications such as mobile phones
- Parents are aware of how to control their child's online experiences
- Parents are aware of new technologies and how to both manage and monitor their children's exposure and use of online technologies and electronic devices.

Approach

At Alamiyah, our e-safety education starts with the parents of the early years pupils. Exploring E-Safety issues and providing information and strategies to ensure that children use these technologies safely and responsibly will be provided to parents:

- The setting will provide parents with guidance in order to support the safe use of screens and online and electronic devices
- Filtering and controls for staff and pupil computers are in place to minimise or eliminate the risk that inappropriate material can be accessed.

The Designated Safeguarding Lead is responsible for online safety concerns. All concerns need to be raised as soon as possible to **Nasima Bobat.**

Pupil Online Safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers the setting to protect and educate the setting in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

- **Contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

The safeguarding policy has further information regarding this.

Online Child on Child Abuse

Children can abuse other children online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content. This is very serious and must be appropriately handled. For information, *see section on Child on Child Abuse and Managing Allegations against other pupils in the Safeguarding Policy.*

Managing Information Systems

Pupils ICT equipment, Electronic Devices and Internet access

- Pupils do not have access to the internet or any electronic devices connected to the internet.
- If pupils are working do work with any device linked to an ipad or computer, they will be supervised at all times
- The designated person has overall responsibility for ensuring that children and young people are safeguarded and risk assessments, in relation to online safety, are completed.
- Appropriate content blockers and filtering controls will be applied to all devices, including ipads and computers and the network so that inappropriate material is not accessible.
- Monitoring all internet usage across the setting

- Ensuring all devices are password protected and have screen locks. Practitioners are reminded to use complex strong passwords, keep them safe and secure, change them regularly and not to write them down
- Providing secure storage of all of the organisation's devices at the end of each day
- Ensuring no social media, messaging or gaming apps are installed on the organisation's devices
- Children are taught the following stay safe principles in an age appropriate way for example in the early years

1. only go online with a grown up
2. tell a grown up if something makes me unhappy when online

- Talking to children about 'stranger danger' and deciding who is a stranger and who is not; comparing people in real life situations to online 'friends'
- When using online video chat, such as Zoom, Teams, Skype, FaceTime etc. (where applicable) discussing with the children what they would do if someone they did not know tried to contact them
- The designated person will also seek to build children's resilience in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age appropriate ways.
- Staff report any suspicious, offensive or inappropriate material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.
- Suspicions that an adult is attempting to make inappropriate contact with a child online will be reported to the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk.
- The designated person ensures staff have access to age appropriate resources to enable them to assist children to use the internet safely.
- If staff become aware that a child is the victim of cyberbullying, they follow the anti bullying policy and procedure and can also refer parents to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or www.childline.org.uk.
- Using tracking software to monitor suitability of internet usage (for older children)

Pupil Use of Mobile phones

- Pupils do not bring mobile phones or other ICT devices with them to the setting. If a pupil is found to have a mobile phone or ICT device with them, this is removed and stored in a safe until the parent collects them at the end of the session.

Staff use of ICT Equipment and Electronic Devices

- Only ICT equipment belonging to the setting will be used by staff
- The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose
- All devices and computers have appropriate antivirus and anti spyware protection installed.
- The designated person ensures that settings ensure that inappropriate material cannot be accessed
- Staff do not permit visitors, third party contractors and parents private access to the setting Wi-Fi. There is a secure guest wifi that all visitors can use
- If a second hand computer is purchased or donated to the setting, the IT staff will wipe and reset the computer to ensure that no inappropriate material is stored on it.
- Staff do not to use personal electronic devices with imaging and sharing capabilities, including mobile phones, smart watches and cameras
- Staff will be provided with training, at least annually, in online safety and understanding how to keep children safe online. We encourage staff and families to complete a free online safety briefing, which can be found at https://moodle.ndna.org.uk/
- Staff model safe practice when using technology with children and ensuring all staff abide by an acceptable use policy such as instructing staff to use the nursery IT equipment for matters relating to the children and their education and care only. No personal use will be tolerated (see Acceptable internet use policy)
- Staff protect the digital reputation, including the appropriateness of information and content that is posted online, both professionally and personally. This is continually monitored by the setting's management

- Staff must not friend or communicate with parents on personal devices or social media accounts
- Staff ensure that all electronic communications between staff and parents is professional and takes place via the official nursery communication channels, e.g. the setting's email addresses and telephone numbers. This is to protect staff, children and parents
- Staff will signpost parents to appropriate sources of support regarding online safety at home

Staff, Volunteers and Visitors Use of Personal Devices such as Mobile Phones and Smartwatches:

Mobile phones/Smartwatches or any device with imaging and sharing capability:

- Are not used on the premises where the children are present during operating hours and may not be used in the garden area when the children are outdoors.
- Can only be used in the office [when children are not present] or off the premises.
- Are kept in lockers in the office whilst teaching staff are working and the children are on site.
- Visitors are required to place their phones in a secure place in the office building and not use their devices onsite.
- If an organisational mobile phone is used, it will not be a smart phone or the smart-phone features will be disabled so that photos could not be taken and sent from the phone
- During outings, staff must only use mobile phones belonging to the nursery
- Organisation devices will not be taken home with staff and will remain secure at the setting when not in use
- Staff and volunteers ensure that the setting telephone number is known to family and other people who may need to contact them in an emergency so that their personal phone does not need to be used.
- If members of staff or volunteers take their mobile phones on outings, for use in case of an emergency, they must not make or receive personal calls, or take photographs of children

Photographs and Filming

Permission is sought from parents for taking photographs of their child for a variety of purposes. Specific permission is sought if any filming is due to take place on the premises.

Use of Cameras

The setting has several cameras and iPads which are used to take photos of the children for their records and for setting publicity materials.

- These cameras remain at the setting and cannot be taken off site.
- Photos are downloaded at the setting on setting computers.
- Photos cannot be placed on personal electronic devices and taken home.
- Staff must not bring their own personal cameras or video recording equipment into the setting.
- Photographs and recordings of children are only taken for valid reasons i.e. to record their learning and development or for displays within the setting.
- Where parents request permission to photograph or record their own children at special events, general permission is gained from all parents for their children to be included. Staff may produce group photographs to distribute to parents on request. In this case we will gain individual permission for each child before the event. This will ensure all photographs taken are in line with parental choice. We ask that photos of events such as Eid parties are not posted on any social media websites or other platforms without permission from the parents of all the children included in the picture
- If photographs of children are used for publicity purposes, parental consent must be given and safeguarding risks minimised, for example, ensuring children cannot be identified by name or through being photographed in a sweatshirt with the name of their setting on it. Those photos remain the property of Alamiyah and are downloaded to the setting network.

Use of Online Learning Journal and Data Management System

The setting uses a website-based system called My Montessori Child for administrative and record-keeping purposes, including taking the attendance register, making text-based and

photographic records of children's activities, planning lessons, reviewing children's progress, and compiling statutory Department for Education reports. Data and photographs are uploaded into the My Montessori Child system by teachers using Internet-connected Apple iPads at the setting. Data and photographs stored remotely on My Montessori Child's online servers are protected by industry-standard Internet security procedures including encrypted transmission, passwords, access-device registration and physical protections. The system administrator of My Montessori Child who has access to the children's data and photographs on a need-to-know basis has been subject to an Enhanced Disclosure and Barring Service (DBS) check (Disclosure number 001382556238). My Montessori Child is registered in accordance with the Data Protection Act and GDPR with the Information Commissioner's Office (Registration Z3311745).

Physical location of iPads at Alamiyah

The iPads are stored securely and out of reach of pupils. No iPad may be used in toilets or nappy-changing areas. Teachers must behave responsibly with iPads as pieces of delicate electrical equipment, protecting them from damage and ensuring they pose no physical risk to children in the setting.

Uploading of photos to the Internet

Photos stored on the iPad are never uploaded to any part of the Internet except to a secure online journal. For example, no photo of any child or group of children on the iPad may be e-mailed, posted to Facebook, tweeted on Twitter, or pinned to Pinterest. Even parent requests to e-mail photos from an iPad are always refused for security reasons. In order to ensure that no photos are being uploaded, e-mail 'sent' lists and web histories on the iPad are never cleared so that they may be checked by the manager.

iPad Restrictions

All iPads used in the setting have PIN-protected 'Restrictions' on web content and apps.

In Settings > General > Restrictions, these settings are used:

- Facetime, Installing apps and Deleting apps are OFF
- Allowed Content is restricted (using United Kingdom ratings) as follows: 'Clean'

Music & Podcasts, Apps

- In-App purchases are ‘OFF’, and Require Password is set to ‘Immediately’
- In the Games Centre, Multiplayer Games and Adding Friends are set to ‘Off’.

We carry out routine checks to ensure that emails and text messages (where applicable) have not been sent from these devices.

Any teacher has a right to challenge any other teacher regarding their iPad use and is obligated to report any concern immediately to the setting’s Designated Safeguarding Lead. We also remind staff of the Whistleblowing policy if they observe any member of staff breaching these safeguarding procedures. For more information, please refer to the setting’s Safeguarding Policy and Whistleblowing Policy.

Use of the Internet, Email and Social Networking Sites

Staff are advised to manage their personal security settings to ensure that their information is only available to people they choose to share information with.

Staff should not accept service users, children and parents as friends on personal social networking due to it being a breach of expected professional conduct. On professional networks and for professional purposes this type of use is permitted.

Staff avoid personal communication, including on social networking sites, with parents with whom they act in a professional capacity. If a practitioner and family are friendly prior to the child coming into the setting, this information is shared with the Manager prior to a child attending and a risk assessment and agreement in relation to boundaries is agreed.

In the event that staff name the organisation or workplace in any social media they do so in a way that is not detrimental to the organisation or its service users.

Photo permission must be sought if a child’s photo is to be used on the setting website or in brochures and publicity materials.

Staff observe confidentiality and refrain from discussing any issues relating to work. Staff should not share information they would not want children, parents or colleagues to view.

Staff should report any concerns or breaches to the designated person in their setting.

Personal data, incidents or events that occur at the setting may not be published on the internet, social networking sites or sent on email except with permission. Information or data that must not be published includes any information that may cause distress to those involved or breach the terms of conduct outlined in the confidentiality policy.

ONLY Official organisation Email addresses may be used to send sensitive data to authorised personnel such as financial data or pupil data.

This includes the names of children, staff or parents and any other data, which may identify a child, parent or staff member.

Photos of the setting premises or staff on the premises or children MUST NOT be published anywhere on the internet and particularly on social networking sites, except on the Montessori record keeping software which is accessed only by passwords used by authorised staff only.

Electronic learning journals for recording children's progress

- A risk assessment is conducted with details on how the learning journal is managed to ensure children are safeguarded.
- Staff adhere to the guidance provided with the system at all times.
- Strong passwords are used to enter the system and staff lock screens after use

Use and/or distribution of inappropriate images

- Staff are aware that it is an offence to distribute indecent images. In the event of a concern that a colleague or other person is behaving inappropriately, the Child Protection Procedure, in relation to allegations against staff and/or responding to suspicions of abuse, is followed.

- Staff are aware that grooming children and young people online is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above). Further guidance:

How will published content be managed?

- The contact details on the website will be the setting address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- E-mail addresses will be published carefully, to avoid spam harvesting.
- The website will comply with the setting's guidelines for publications including respect for intellectual property rights and copyright.

Can pupil's images or work be published?

- Images that include pupils will be selected carefully and will not be identified by name.
- Pupils' full names will not be used anywhere on the website in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.
- Work can only be published with the permission of the pupil and parents.

Reporting Concerns

If any concerns arise relating to online safety, then we will follow our Safeguarding children and child protection policy and report all online safety concerns to the DSL.

The DSL will make sure that:

- All staff know how to report a problem and when to escalate a concern, including the process for external referral
- All concerns are logged, assessed and actioned in accordance with the setting's safeguarding procedures
- Parents are supported to develop their knowledge of online safety issues concerning their children

- Parents are offered support to help them talk about online safety with their children using appropriate resources
- Parents are signposted to appropriate sources of support regarding online safety at home and are fully supported to understand how to report an online safety concern
- Staff have access to information and guidance for supporting online safety, both personally and professionally

Cyber security

Good cyber security means protecting the personal or sensitive information we hold on children and their families in line with the Data Protection Act. We are aware that cyber criminals will target any type of business including childcare and ensure all staff are aware of the value of the information we hold in terms of criminal activity, e.g. scam emails. All staff are reminded to follow all the procedures above including backing up sensitive data, using strong passwords and protecting devices to ensure we are cyber secure.

To prevent any attempts of a data breach (which is when information held by a business is stolen or accessed without authorisation) that could cause temporary shutdown of our setting and reputational damage with the families we engage with, we inform staff not to open any suspicious messages such as official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries'.

Staff are asked to report these to the manager as soon as possible and these will be reported through the National Cyber Security Centre (NCSC) Suspicious email reporting service at report@phishing.gov.uk

How will information systems security be maintained?

- The security of the setting information systems will be reviewed regularly.
- Antivirus and anti spyware protection will be updated regularly.
- Security strategies will be discussed and implemented.

- Portable media may not used by anyone staff and non-staff members without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed
- Files held on the setting's network will be regularly virus-checked.
- The Computing subject leader/ IT Technician / network manager will review system capacity regularly.

Addendum: Safe Remote Teaching

Parent Communications

The setting acts as partners with parents and carers to reinforce the importance of children being safe online. Parents and carers are informed about the systems the setting uses to filter and monitor online use. Parents are provided with information about online safety and resources. Parents and carers are made aware of what their children are being asked to do online, including any sites that they will be asked to access and be clear who from the setting their child is going to be interacting with online.

Keeping Pupils Safe Online during Remote Learning

The setting recognises:-

- the increased use of online technologies when learning remotely
- the wide-range of content which is available to children via the internet
- that alongside the benefits of technology, there are also risks

In response to these risks during periods of remote working and distance learning, the setting has put in place an IT Support team as a contingency should a single member of the IT staff become unavailable. Staff are trained with the appropriate technical knowledge to maintain safe working arrangements.

We recognise that increased time online will pose increased risk to children, including but not limited to:-

• Grooming

• Exploitation, both criminal and sexual

• Radicalisation

• Child on child abuse, including cyber-bullying

• Sexual harassment

All staff who interact with pupils, including during remote interactions, will continue to be vigilant and look out for signs that a child's safety and welfare might be at risk. Staff are trained on the key safeguarding issues which can be found in 'Keeping Children Safe In Education'.

Keeping Staff Safe Online

Staff and volunteers continue to work in line with the setting's policy and procedures on online safety, the staff code of conduct and IT acceptable use policy. When learning remotely, parents and pupils will only be contacted via a setting family email account which is monitored and subject to an acceptable user agreement.

When staff are conducting live lessons with pupils, it is important to ensure that a parent or carer above the age of 18 is present in the room within the sight and hearing of the teacher and child. Staff must check that this is the case before starting the lesson. If there is no other adult present with the child then the parent should be called and the lesson will have to be abandoned until suitable supervision is arranged.

Staff will only use email and online voice calls, using organisation accounts that are monitored. They will arrange meetings via online video or voice call using an organisation email address. Staff will not use personal social media, messaging or personal phones to contact parents or pupils.

Staff working remotely should not record any personal information about families or confidential information via personal devices. Where telephone calls are being made by staff working remotely, these should be made using a work phone where possible.

If emails containing personal information/confidential information are being sent remotely, staff

should be reminded to password protect these before sending (and send the password via text or some other platform) or encrypt the email before sending.

Where live lessons or video meetings are being recorded, all parties should be made aware and this should be in line with the setting's data protection guidance. The data protection officer should be made aware.

Further guidance for staff working remotely can be found in the Safer Working Practice addendum (published in April 2020).

Staff Protocol for Remote Learning

Teachers who deliver online learning to pupils must adhere to the following:

● At the start of the session you should greet the child

● A desktop or a laptop should be used to deliver online learning.

● Laptops should be positioned on a table. If you deliver your online learning from your home please position your equipment on a table or surface in a room that has a professional background (does not have a bed or look like a private space).

Please ensure that your background looks professional and clear. There

should be no political or inappropriate images or items in your background. You may wish to

use a pre-loaded background or blur out the background.

● Both pupil and staff video function must be enabled throughout the whole session.

Headphones should be worn for the child's privacy.

● The teacher will unmute the pupil when they wish for the child to talk/interact/recite within

the session. Do inform the child that you are unmuting them.

● If you are working from home, please ensure that you are in a separate room from other

family members so that they do not appear during the session.

● Both pupil and staff members are to remain seated throughout the session.

● If working from home, please wear professional attire just as you would on a regular

Working day. Please refer to our Operational Manual for the staff dress code.

● You must communicate and attend lessons arranged through your formal organisation email address only.

If you experience any technical issues either alert the teacher overseeing your lesson or call

the setting landline on 020 8595 5999 or contact admin or IT support on

admin@alamiyahschool.org or itsupport@alamiyahschool.org for assistance.

Parent and Pupil Online Learning Protocol

Parents will also be emailed out a pupil online learning protocol which they have to agree to to ensure that pupils are safeguarded as far as possible. The protocol stipulates that parents must ensure that:

- pupils are dressed appropriately
- they are seated in a communal area of the house rather than a bedroom
- Their device or computer is positioned on a table with the camera angled at the child's face so that the camera does not capture any inappropriate images
- that they are supervised at all times

Review

This policy will be reviewed annually or sooner or if there is any change in statutory guidance or legislation. See 'Policy Review Schedule'.

Last Reviewed: 07/09/2026

Adopted in a meeting at Alamiyah Montessori on 08/09/2025

Signed by Nasim Bobat (Manager) and S Motara (Nominated Person)

on behalf of Alamiyah Montessori

With reference to -

Keeping Children Safe in Education (Sept 2026)

Early Years Foundation Stage (EYFS) Statutory Framework 2026

Data Protection Act 2018, GDPR 2018