E-Safety Policy

With reference to -

Keeping Children Safe in Education (Sept 2022)

The Education (Independent School Standards) Regulations 2014

Early Years Foundation Stage (EYFS) Statutory Framework 2021

Racial and Religious Hatred Act 2006

Sexual Offences Act 2003

Communications Act 2003 (section 127)

Data Protection Act 2018, GDPR 2018

The Computer Misuse Act 1990 (sections 1 – 3)

Malicious Communications Act 1988 (section 1)

Copyright, Design and Patents Act 1988

Public Order Act 1986 (sections 17 – 29)

Protection of Children Act 1978 (Section 1)

Obscene Publications Act 1959 and 1964

Protection from Harassment Act 1997

Regulation of Investigatory Powers Act 2000

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, handheld devices and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for children and young people. In addition, there is information on weapons, crime and racism which would have restricted access elsewhere. Pupils must also learn that publishing personal information cannot later be retracted and could compromise their security and that of others.

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 school pupils do not use online technology in the lower and middle school they are prepared to use technology in the upper school from Year 5/6 onwards. Prior to Year 5, pupils are screen free, and use offline technologies to build their understanding of the mechanics of the world before being provided with online technology as a learning aid when they have mastered the basics of book based research and pencil and paper skills. Staff may if appropriate provide pupils with planned and supervised access to an intranet prior to Year 5. We are also aware that pupils are likely to have some access to technology at home or at the homes of friends, family and relatives prior to year 5/6. It is therefore important that all pupils and parents are inducted into e-safety by the school.

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, young people and vulnerable adults 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
- pupils are aware of how to control their online experiences

- parents are aware of new technologies and how to both manage and monitor their children's use of online technologies and electronic devices.

Approach

At Alamiyah, our e-safety education starts at year 2 with the very basics and continues throughout a pupil's school life. Exploring E-Safety issues and providing information and strategies to ensure that pupils use these technologies safely and responsibly will form part of pupils Technology and SMSC curriculum.

- The school will provide parent workshops and guidance on e-safety in order to support the safe use of online and electronic devices at school and in the home.
- Filtering and controls for staff and pupil computers are in place to minimise or eliminate the risk that inappropriate material can be accessed.
- Pupils at the school will be supervised and closely monitored when using any electronic or online technology to ensure that any issues with the filtering and controls are flagged up immediately.
- Pupils will also be educated about the benefits, risks and harm that comes from using these technologies.
- Pupils will also being taught how to evaluate information which they access online so that they can be more critical and discerning about what they are presented with. This will also assist pupils to stay safe online so that they do not easily fall prey to online scams and other predatory behaviour.

Staff will report any e-safety issues to the E-Safety Officer, (and also the Designated Safeguarding Lead if the issue raises safeguarding concerns).

Why is Internet use important?

- The purpose of internet use in school is to to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions
- The Internet is an essential element in 21st century life for education, business and social interaction.
- Pupils at the school do not use the internet before the age of 9-10 years old. However we do understand that pupils may use the Internet outside school and will

need to learn how to evaluate information on the internet and to take care of their own safety and security.

How will pupils learn how to evaluate Internet content?

- The school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials will be an integral part of lessons where online materials are used.

Managing Information Systems

Pupils ICT equipment, Electronic Devices and Internet access

- Pupils do not have unsupervised access to the internet.
- If pupils require information from the internet prior to Year 5, then a staff member will provide assistance to search for items so that their usage can be supervised fully.
- 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 filtering and controls will be applied to all computers/network at the school so that inappropriate material is not accessible.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Children are taught the following stay safe principles in an age appropriate way prior to using the internet;
    1. only go online with a grown up
    2. be kind online
    3. keep information about me safely
    4. only press buttons on the internet to things I understand
    5. tell a grown up if something makes me unhappy on the internet

- 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.
- If a second hand computer is purchased or donated to the school, the designated person will ensure that no inappropriate material is stored on it before children use it.
- All computers for use by children are located in an area clearly visible to staff.
- Children are not allowed to access social networking sites.
- Staff report any suspicious or offensive 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.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- At an appropriate age pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

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 school to protect and educate the whole school 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.

Children are taught about safeguarding, including online safety. *The safeguarding policy has further information on 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.*

Safe Remote Teaching

Parent Communications

The school 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 school 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 school their child is going to be interacting with online.

Keeping Pupils Safe Online

The school 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 school 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. Further guidance to keep pupils and staff safe when working remotely can be found in the Safer Working Practice addendum (published in April 2020). Staff are trained on the key safeguarding issues which can be found in Annex A of 'Keeping Children Safe In Education' (Sept 2022) In addition, pupils are sign-posted to age appropriate practical support should they have worries or concerns whilst online. Links to support can be found below :-

UK Safer Internet Centre Helpline: https://www.saferinternet.org.uk/our-helplines

Child Exploitation and Online Protection Centre: https://www.ceop.police.uk/safety-centre/

Parentzone: https://parentzone.org.uk/

Keeping Staff Safe Online

Staff and volunteers continue to work in line with the school'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 school 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 school accounts that are monitored. They will arrange meetings via online video or voice call using a school 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 school'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

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

● You must communicate and attend lessons arranged through your formal school email

address only.

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

the School 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 pupil's are safeguarded as far as possible. The protocol stipulates that parents must ensure that:

- pupils are dressed appropriately
- they are seated in an 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

Pupil Use of Email

- Children are not permitted to use personal email in the school. Parents and staff are not normally permitted to use school equipment to access personal emails.
- Staff do not access personal or work email whilst supervising children.

Pupil Use of Mobile phones

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

Staff ICT equipment and Electronic Devices

- Only ICT equipment belonging to the school will be used by staff and pupils.
- The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.

- All computers have virus protection installed.
- The designated person ensures that safety schools are set to ensure that inappropriate material cannot be accessed.

Use of Personal Mobile Phones:

Mobile phones:

- Are not used on the premises where the children are present during school 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 mobile phones onsite.
- If the school were to use a mobile phone, smart-phone features would be disabled so that photos could not be taken and sent from the phone.
- Staff and volunteers ensure that the school 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 school has several cameras and iPads which are used to take photos of the children for their records and for school publicity materials.

- These cameras remain at the school and cannot be taken off site.
- Photos are downloaded at the school on school 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 school.
- Photographs and recordings of children are only taken for valid reasons i.e. to record their learning and development or for displays within the school.
- 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. Parents are advised that they do not have a right to photograph anyone else's child or to upload photos of anyone else's children.
- 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 school on it.

Use of Electronic Devices to Store Data

The school has a number of storage devices, which are school property and cannot be taken off site.

These devices include

- A network server (stores all electronic data centrally)
- 1 terabyte external hard drive
- A USB storage device.

Photos and sensitive data can be placed on these devices to back up data and to transfer files between school computers.

All electronic files which contain sensitive data are locked with password protection.

Extremely sensitive data will also be encrypted. When the school has data of this nature it is subjected to encryption.

Use of IPad Policy

The school 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 school. 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 in the School

The iPads are stored securely in the school's locked office. 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 school.

Uploading of photos to the Internet

Photos stored on the iPad are never uploaded to any part of the Internet except to My Montessori Child. 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 a Head teacher.

iPad Restrictions

All iPads used in the school 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'.

CHILDREN ARE NOT PERMITTED UNATTENDED USE OF IPADS.

Any teacher has a right to challenge any other teacher regarding their iPad use and is obligated to report any concern immediately to the school's Designated Safeguarding Lead. At the discretion of the Designated Safeguarding Lead, the suspected teacher may be required to leave the school immediately and their iPad retained for further investigation. For more information, please refer to the School's Safeguarding 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 school, this information is shared with the Headteacher 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 School 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 school.

Personal data, incidents or events that occur at the school 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 School 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 school 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

- The Headteacher seeks permission from the Principal/Governors prior to using any online learning journal.
- A risk assessment is completed 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.

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 information systems security be maintained?

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed and implemented.

- Portable media may not used by children and non-staff members without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly virus-checked.
- The Computing subject leader/ IT Technician / network manager will review system capacity regularly.

How will email be managed?

- Pupils may only use approved e-mail accounts.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- ***For external e-mail linked to class work, when contacting other schools and outside agencies, whole-class or group e-mail addresses will be used.***
- Where practicable, access in school to external personal e-mail accounts, including webmail accounts, will be blocked.
- Excessive social e-mail use can interfere with learning and will not be allowed.
- E-mails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

How will published content be managed?

- The contact details on the website will be the school 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 head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website will comply with the school'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.

How will social networking and personal publishing be managed?

- Where feasible the school will endeavour to block access to social networking sites.
- Newsgroups will be blocked to children and non-staff members unless a specific use is approved by a member of staff.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, social networking details, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the pupil or his/her location eg. house number, street name or school.
- If applicable, teachers' official blogs or wikis should be password protected and run from the school website. Teachers will be advised not to run social network spaces for pupil use on a personal basis.
- Pupils will be advised on security and encouraged to set secure passwords, deny access to unknown individuals and instructed how to block unwanted communications. pupils will be encouraged to invite known friends only and deny access to others.
- pupils will be advised not to publish specific and detailed private thoughts.

How will filtering be managed?

- If staff or pupils discover unsuitable sites, the URL must be reported to the appropriate member of staff in the school.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- Any material that the school believes is illegal must be reported to appropriate agencies such as Internet Watch Foundation (IWF) or Child Exploitation and Online Protection Centre (CEOP) (addresses later).
- Websites that pupils access will be recorded and monitored regularly
- The UK Safer Internet Centre has published guidance as to what “appropriate” filtering and monitoring might look like: UK Safer Internet Centre: appropriate filtering and monitoring. South West Grid for Learning (swgfl.org.uk) have created a tool to check whether a school or college’s filtering provider is signed up to relevant lists (CSA content, Sexual Content, Terrorist content Your Internet Connection Blocks Child Abuse & Terrorist Content).The NSPCC also provide helpful advice.

How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used in any classroom and are prohibited on the school site except for the office. In the event of an emergency, a school mobile phone with no smart phone, wifi or camera will be used in an emergency. The sending of abusive or inappropriate text messages is forbidden.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. (See Data Protection Policy)

Policy Decisions

How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school’s electronic communications.
- All staff must read and sign for the Staff Handbook, **ICT Acceptable Use Agreement** and the E-Safety Policy before using any school IT resource.
- During Years 2-4, occasional access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials.

- During Years 5-6, access to the Internet will be with adult supervised access to specific, approved online materials
- Parents will be asked to sign and return a consent form for pupil access.
- Parents will be informed that pupils will be provided with supervised Internet access

How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit IT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will E-Safety complaints be handled?

- Complaints of pupil internet misuse will be dealt with by the Headteacher
- Any complaint about staff misuse must be referred to the Headteacher/DSL/LADO.
- Any complaint about misuse by a headteacher must be referred to the Principal.
- Any complaint about misuse by the Principal must be referred to the Board of Governors
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the local Police when handling potentially illegal issues.
- Sanctions within the school discipline policy include:
    - interview/counselling by the headteacher;
    - informing parents or carers;
    - removal of internet or computer access for a period.

How is the Internet used across the community?

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Communication of E-Safety

How will the policy be introduced to pupils?

- E-Safety rules will be posted in areas with Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede internet access.

How will the policy be discussed with staff?

- All staff will be given access to the School E-Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential.
- Staff or contractors that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible internet use and on the School E-Safety Policy will be provided as required.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school's E-Safety Policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use and or workshops on e-safety.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed below in E-Safety Contacts and References.

Legal Framework

Notes on the legal framework

This section is designed to inform users of legal issues relevant to the use of electronic communications. It is not professional advice.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

- The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the child to 18 years old;
- The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and
- The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 2018

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).
- UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.
It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Notes

Using the Internet to support learning

Most Internet use in primary schools is safe, purposeful and beneficial to learners. There is always an element of risk: even an innocent search can occasionally turn up links to adult content or violent imagery. Risks are magnified by the upsurge in schools’ Internet access. However, many teachers feel that there is a far greater problem in the amount of irrelevant, incomprehensible material typically yielded by Internet searches. For the youngest pupils, the greatest risk is through inadvertent access. Fast broadband means that inappropriate images can appear almost instantaneously. Children can innocently follow a series of links to undesirable content. A procedure should be agreed with all staff on what to do, and how to handle the situation with pupils. For example: *Close or minimise the image or window immediately. Don't try to navigate away. If pupils saw the page, talk to them about what has happened, and reassure them. Later, investigate the history of visited sites and how the pupil got there.* In view of the risks, we advise that primary pupils are supervised at all times when using the Internet.

Search engines

The BBC search engine is a safer approach for children: http://www.bbc.co.uk/search
Image searches are especially risky. There may be no need for pupils to download them, as long as an adult downloads the images before the lessons and stores them in a shared folder. Alternatively, teachers may use Microsoft's clipart library, which automatically adds downloaded images to Clipart: http://office.microsoft.com/clipart/
Please note that NO filter-based search engine is completely safe.

Curriculum planning

Good planning and preparation is critical in ensuring a safe starting point for the development of Web search skills and strategies. Tasks can be planned that do not require an Internet-wide search engine.

If the aim is to teach search skills, **BBC Schools** offers a safe environment. The search box automatically restricts the search to the BBC Schools site. There is no indication of age range, but pupils can judge readability from the example retrieved by the search www.bbc.co.uk/schools. Importantly, primary pupils can learn skills such as keyword selection to narrow down searches, and evaluating quality and relevance. This will prepare them for efficient, productive Internet research in the secondary phase.

Webquests contain direct links to support research. There is no need to use a search engine. Some webquests simply consist of a list of questions. The questions are linked directly to text sources and offer a motivating means of engaging reluctant readers in 'finding out'.

Any teacher able to produce a document in Word can create his/her own webquest. To place an active web link on the page, simply select and copy from the address bar in Internet Explorer, and paste into Word. To follow the link, press and hold the Ctrl key while you click on the link. Primary school learners need not be exposed to the risks of the unfenced Internet!

E-Safety Contacts and References

BBC WebWise

http://www.bbc.co.uk/webwise/0/

Childline

http://www.childline.org.uk/

Child Exploitation & Online Protection Centre

http://www.ceop.gov.uk

NSPCC

https://www.nspcc.org.uk/

Grid Club and the Cyber Cafe

http://www.gridclub.com

Internet Watch Foundation

http://www.iwf.org.uk/

Internet Safety Zone

http://www.internetsafetyzone.com/

Kidsmart

http://www.kidsmart.org.uk/

Stop Text Bully

www.stoptextbully.com

Think U Know website

http://www.thinkuknow.co.uk/

ChildNet

http://www.childnet.com/

UK Safer Internet

http://www.saferinternet.org.uk/

Get Safe Online

http://www.getsafeonline.org/

Guidance on Cyberbullying

https://www.childnet.com/parents-and-carers/hot-topics/cyberbullying

UK Council for Child Internet Safety

https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Review

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

Adopted in a meeting at Alamiyah School on 14/07/2017

Signed: H Musa (Headteacher) and S Motara (Chair of Trustees)