Bismilahir-Rahmanir-Rahim

IQRA SLOUGH ISLAMIC PRIMARY SCHOOL (ISIPS)

IT Usage

We Learn, We Lead, We Inspire

Review Date..... 1st September 2023 .....

Signature..... .....

Frequency of Review.....Annually.....

Next Review Date..... 1st September 2024 .....

IT Usage Policy

The general principles of this policy are to ensure that Iqra Primary School's IT systems and infrastructure remain stable and secure. Whilst the following points are in part prescriptive, any action by a person(s) that interfere with the safe, secure and optimal running of the IT systems in the School will be deemed as misuse and dealt with accordingly.

The following rules are contractual obligations, mandatory for all employees, and contractors when using the School's IT systems. Any breach of these rules may result in the application of disciplinary procedures, and could give rise to criminal and/or civil liability.

The School's systems comprise all or any part of the computers, software, peripherals, infrastructure, storage media and the information they contain provided by or on behalf of the School for the conduct of its business irrespective of how they are accessed.

All those accessing or using these systems have a general responsibility only to act in a way that is lawful. The Computer Misuse Act (1990) creates three specific criminal offences, namely;

- unauthorised access to computer material e.g. "hacking", exceeding authorised access,
- unauthorised access to a computer system with intent to commit or facilitate the committing of a further offence e.g. theft by redirecting funds from someone else's account; and
- unauthorised modification of computer material e.g. deliberate deletion or corruption of programs or data.

In particular, users **MUST NOT:-**

- access a computer system or computer held information and data without proper authority,
- make unauthorised modifications to the contents of any computer system, including deleting or changing data ,
- make unauthorised modifications to the configuration of any part of any computer system,
- install any software on to a School system without the proper authority,
- take any action to circumvent any security measure implemented within the systems or
- make or use, or permit others to make or use, unauthorised copies of computer software, including associated documentation and back-up copies

All those accessing or using school systems **MUST:-**

- ensure that any information under their control that is confidential, critical, commercially sensitive, or may have contractual or other legal implications for the School remains secure
- use only properly licensed software, complying with the conditions of the license at all times

Users must not download on to School equipment and/or systems, any unauthorised software whether licensed or not.

Offensive and/or inappropriate material must not be stored on any of the School's IT equipment, including servers, PCs, tablet or laptops, nor should the equipment and systems be used to access and read such material.

It is recognised that there will be limited occasions where individuals may need to use the systems for personal rather than business purposes. Such use is authorised, with the exception of accessing personal email accounts. These accounts include: but are not limited to; Hotmail, Yahoo, Tiscali, BT Internet etc. Such use of the system may result in the application of the disciplinary procedure.

If an individual is in doubt regarding accessing an external site, they should contact the Business Manager.

The use of School systems for limited personal use is authorised, with the exception of the above, provided it does not:

- impact on an individual's working time,
- interfere with the performance of work duties, or
- impact on the performance of School systems.

In order to ensure the integrity and legality of its systems, the School reserves the right to monitor and read all information held on those systems. This includes, but is not limited to, all activity logs, documents, data sets and all traffic to, and from or within those systems.

11 Use of E-mail

When using the School's e-mail system internally or externally, individuals may not send any e-mail, and/or attachment which:

- contains information that is confidential, critical, commercially sensitive, or may have contractual or other legal implications for audit, without appropriate authorisation
- may damage the School's reputation or its relationship with its partners, or which may embarrass the School or its partners
- makes representations or expresses opinions purporting to be those of the School, without appropriate authority

- is illegal, defamatory, obscene, pornographic, offensive, or which may be considered by others to cause distress or to constitute sexual, racial or other harassment or discrimination
- may infringe copyright
- knowingly introduces a virus or any other form of malicious software to any School or partner network
- constitutes 'junk' or 'chain' e-mail
- is for private commercial purposes unrelated to the School

In addition, even where none of the above categories are involved, where an individual has excessive amounts of personal e-mail traffic on their system, this may also be treated as a disciplinary offence.

1.2 Use of Internet and Website Browsing

Individuals accessing any system external to the School (including but not limited to the Internet) using School equipment may not, under any circumstances, access websites which are or may be:

- illegal, defamatory, obscene, pornographic, offensive
- considered by others to cause distress or to constitute sexual, racial or other harassment or discrimination otherwise inappropriate in the workplace

Individuals may not use modems to access the Internet or any other networks in order to bypass School security measures designed to protect the School from those networks.

The School reserves the right to monitor websites being accessed by users, for the purpose of ensuring that these rules are adhered to.

1.3 Passwords

Passwords are the principal security mechanism to prevent unauthorised access to the School's computer systems and information. Employees / workers are contractually accountable for all use of the IT systems under their individual identity, and hence need to protect their password from abuse by others.

Although set by individuals, passwords remain the property of the School and any passwords used in the system must be disclosed immediately if demanded by the Head Teacher or Business Manager.

Under no other circumstances must any password be disclosed.

If an individual becomes aware of any password that is not their own, they must notify the Business Manager within 24 hours.

1.4 Laptops

Employees who possess a School laptop or who have temporary use of a 'pool' laptop are responsible for its safe keeping and in the event of loss, may be

responsible for the cost of its replacement. If laptops are taken out of the School they must be kept secure at all times. When carried in a car, they should be kept out of sight, in the boot. Laptops must not be left in cars overnight or during the course of the day when the car is left unattended. The School reserves the right to seek compensation if the security measures are not observed. Staff will be issued with a letter outlining their responsibilities whilst School equipment is in their possession. Staff members will need to sign to confirm their agreement to the terms.

1.5 Peripherals

At no time should a member of staff attach, by any means, any peripherals to School systems for personal use. These peripherals include but are not limited to; Ipods, MP3 players, USB keys, cameras, bluetooth devices personal organisers, mobile telephones etc.

The use of approved USB keys and other mass storage devices for business purposes only is permitted, when using approved devices / hardware.

Where an individual is in doubt regarding the use of a peripheral, they should contact the Business Manager

1.6 Storage of Equipment

Year Leaders are responsible for the security and monitoring of laptops allocated to their Year Group (see point 2.3 Resources below). It is the responsibility of Year Leaders to:

1.6.1 Ensure laptop trolleys are kept locked when not in use.
1.6.2 Ensure trolleys are locked at the end of each day/during school holidays.
1.6.3 Ensure all equipment and keys to the trolleys are accounted for.

In signing this policy, you are acknowledging that you have read and understood your responsibilities in relation to IT Usage.

I acknowledge that I have read and understood my responsibilities in relation to IT Usage and confirm that I will comply with the policy as detailed above.

Signed: _____

Print Name: _____

Date: _____

Teaching and Learning

2.1 Safeguarding:

Iqra acknowledges the important role that the curriculum can play in the prevention of abuse and in the preparation of our pupils for the responsibilities of adult life and citizenship. It is expected that all curriculum coordinators will consider the opportunities that exist in their area of responsibility for addressing the 'Keeping Children Safe in Education: Statutory guidance for schools and colleges April 2014'. As appropriate, the curriculum will be used to build resilience, help pupils to keep safe and to know how to ask for help if their safety is threatened.

All computer equipment and internet access within the school will be subject to appropriate "parental controls" and Internet Safety Rules (more information can be sought from the Computing and E-safety policy).

2.2 Internet Safety

Internet access is planned to enrich and extend learning activities. The school has acknowledged the need to ensure that all pupils are responsible and safe users of the Internet and other communication technologies. An acceptable use policy has thus been drawn up to protect all parties and rules for responsible computer use are discussed with each child. The Acceptable Use Policy document is available to all staff on the school shared drive. Although the school offers a safe online environment through filtered internet access we recognise the importance of teaching our children about online safety and their responsibilities when using communication technology. This forms our curriculum in Computing and is discussed openly in other lessons to deepen understanding.

2.3 Resources:

ICT resources are deployed throughout the school to maximise access, to enhance teaching & learning and to raise attainment. To enable regular and whole class teaching of computing the school has provided each year group, from years 1 – 6 with 30 laptops which are stored in two laptop trolleys within their year group. This provides easy access for teachers and pupils to use ICT in any of their lessons. Each laptop has the required software downloaded which are needed to teach to meet the national curriculum standards. All teachers are responsible for ensuring laptops are put back into the allocated trolleys. Each laptop has a coloured sticker at the bottom which indicates which laptop trolley it should be placed in (different for each year group). Laptops should not be shared between year groups as each year group has enough, unless there is an urgent need such as workshop taking place then seek permission from Year Leader. All Year Leaders are responsible for ensuring the correct number of laptops are in each of their trolleys and locked at the end of each day. Year Leaders are accountable for the loss or damage of any of the laptops/trolleys within their year group.

The school works in partnership with the service provider to ensure filtering systems are as effective as possible. If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E Safety co-ordinator. Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.4 Homework:

Online homework is set through Conquer Math's and Literacy Planet. Pupils have their own username and passwords which can be accessed from any school computer, laptop and their own personal computers at home. All teachers have access to their own classes and can set homework accordingly as well as check whether homework has been completed or not. A summary of homework completion is provided through the online websites in to form of charts/ graphs. Phase leaders have admin access which allows them to add new pupils, monitor progress of homework set by teachers and oversee record of homework completion. (See E Safety policy)

2.5 ICT across the curriculum:

The new National Curriculum states that pupils should be taught a range of computer science, information technology and digital literacy. (See computing policy for more detail)

The computing curriculum modules are planned in line with the national curriculum, along with the 'Rising Stars Switched On Computing' scheme and will allow for clear progression. Modules will be followed and adapted to enable pupils to achieve stated objectives. Staff will follow medium term plans from the scheme along with objectives set out in the national curriculum and use the same format for their weekly planning sheet.

Media Suite

To support the cross curricular nature of computing a media suite has been set up where pupils work with an experienced teacher on using professional equipment to film, edit and enhance images using various advanced software and hardware. This goes beyond the national curriculum objectives and expectations.

At least five computers are set up in the media suite to support the more able pupils in KS2 in projects were they learn to code using the Raspberry Pi.

Hand held tablets (GoTab) are deployed to all 3 classes in EYFS to allow pupils to use the basic skills of Paint, listen to stories or music, practice phonics, interact with math games through various apps and collect evidence of their own learning by taking photographs. (See EYFS policy)

Other policies and documents to be read in conjunction with the computing policy:

Acceptable Use Policy

Internet E Safety Policy

Computing Policy

Teaching and Learning Policy

Addendum to Policy – Approved by Governing Body on 23.3.2024

Since the Covid-19 pandemic, remote and hybrid working has brought platforms such as Zoom or Microsoft Teams into common practice to conduct staff, stakeholders, contractors, other agencies and within Schools, parents' meetings. There are principles, expectations, etiquette and policy which should be followed. The purpose of this document is to Outline these, rather than recordings made for teaching and research.
Recordings can be required to be shared as part of a formal information request under the Data Protection Act and Freedom of Information Act, this applies to attendees or any individuals who are included in discussion during the course of the meeting.

Principles
Under no circumstances should covert recordings be taken. This would be a disciplinary offence.
Recordings should not be made as a matter of course they should be considered on the basis of need, individually, due to the complexity, length or if key participants cannot be present for part or all of the duration.
Recordings should not be made without prior consent; the Chair or organiser must notify all attending participants that recording will take place and ask if anyone has any objections. Options should be given to turn camera and or microphone off.
It must be transparently clear that recording is taking place and any joining participants not present at the beginning should be made aware recording is taking place.
Recording must stop at the formal close of the meeting.
On conclusion of the meeting and recording it is appropriate to make the recording available to the participants and give them an opportunity to express any concern on use. This includes sharing, distribution and retention.

Security, Storage and Retention
Obviously, care must be taken with storing recorded data especially confidential recordings. They must be in line with School GDPR Policy. No recordings should be stored on personal devices or USB drives.
Recordings should not be retained for longer than necessary. This would mainly depend on the purpose for making a recording, for instance, once formal minutes or notes have been transcribed recordings should be securely deleted.
No recording should be kept indefinitely.
If a recording is to be shared permission should be requested prior to sharing with non-participants.
As recordings can be subject to Information access requests it is imperative that recordings are made only in exceptional circumstances and that the retention period minimised as much as possible.