Bismilahir-Rahmanir-Rahim

IQRA SLOUGH ISLAMIC PRIMARY SCHOOL (ISIPS)

E-Safety Policy

We Learn, We Lead, We Inspire

Review Date..... 6th August 2019 .....

Frequency of Review.....Annual.....

Next Review Date..... 6th August 2020 ....

Signature..... .....

Iqra Slough Islamic Primary School

Internet E-Safety Policy

Reviewed 6th August 2019

Review Date: 6th August 2020

Acceptable use and Internet E-Safety Policy

Introduction

In school we have access to the internet. This is a powerful tool which opens up new opportunities for everyone and promotes effective learning. We are aware that young people should have an entitlement to safe internet access at all times. However, the school and parents have a duty of care to protect children and ensure that internet use is responsible and safe.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The school's e-safety policy will operate in conjunction with other policies including those for:

Behaviour for Learning
Anti- Bullying
Curriculum
Data Protection
Safeguarding and Child Protection

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

School e-safety policy

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT and for child protection.

- The school's e-Safety Coordinator is also the ICT Coordinator (Mrs Munir, Assistant Head). Mrs Munir works in close co-operation with the named Designated Child Protection Officers of the school and with all SLT.
- Our e-Safety Policy has been written by the school. It has been agreed by the staff and governors.
- E-Safety issues are included in the Child Protection, Health and Safety, Anti- Bullying, PSHE&C and ICT policies.

UNITED NATIONS COVENTION ON THE RIGHTS of the CHILD ARTICLE 13

Children have the right to get and to share information, as long as the information is not damaging to them or to others.

Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their

learning experience.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the school ICT Coordinator.
- Staff should ensure that the use of Internet derived materials by staff and by 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.

Acceptable Use:

Managing Internet Access

Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses broadband with its firewall and filters.

E-mail

- Pupils may only use approved e-mail accounts on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.
- 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.
- E-mail sent to an external organisation 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.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with

photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- Social networking sites, forums and chatrooms will be blocked unless a specific use is approved by the headteacher.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.

Managing filtering

- The school will work 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 coordinator.
- Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- 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 during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff have access to a school phone where contact with pupils is required.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Cyber Bullying

Cyber bullying is when someone uses the internet –often social networking sites, or mobile phones to deliberately upset someone else. To help combat it you can save texts or print out emails and Web Pages. This can be used as proof to catch the bully and stop them.

We take cyber bullying seriously and discuss the issues at school. We tell our pupils and parents the following message: ‘Don’t participate in forwarding pictures, messages or insults about a person. You may think it is a joke, but you could be really upsetting the person involved and even committing a crime. To look at or forward this sort of stuff means you are contributing to cyber bullying. Standing back and letting it happen can be just as bad. If you are worried that someone is getting threatened or hurt by others, offer them support or inform an adult you trust so they can help make it stop. Always respect other people and be aware of what you’re sending and receiving whilst online.’

Policy Decisions

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff (including Teaching Assistants and Supply Teachers) and pupils must read and sign the acceptable ICT Acceptable User Policy (AUP) before using any school ICT resource See Appendix 1-4).
- At FS/Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's Acceptable Use Policy (See Appendix).

Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school can accept liability for the material accessed, or any consequences of Internet access.
- The head teacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

Handling e-safety complaints (see Appendix 5)

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Sanctions within the school discipline policy include:
  - interview/counselling by class teacher / head teacher;
  - informing parents or carers;
  - removal of Internet or computer access for a period.

Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- Parents using school ICT equipment must sign an AUP consent form prior to use (eg Family ICT, Numeracy and Literacy).

Communications Policy

Introducing the e-safety policy to pupils (see appendix 2-4)

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Advice on e-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.

Staff and the e-Safety policy (Appendix 1)

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' / carers' support

- Parents' / carers' attention will be drawn to the School e-Safety Policy in newsletters.

Acceptable use of Mobile Phones

In Iqra Primary School the welfare and well-being of our pupils is paramount. The use of mobile phones in school has been drawn up in the best interests of pupil safety and staff professionalism.

Use of mobile phones

Pupils:

- Pupils are not permitted to have mobile phones at school or on trips
- If in the rare event of a parent wishing for his/her child to bring a mobile phone to school to contact the parent after school:
  - the parent must put their request in writing to the Head teacher
  - the phone must be handed in , switched off, to the secretary's office first thing in the morning and collected from the office by the child at home time (the phone is left at the owner's own risk).
- Mobile phones brought to school without permission will be confiscated and must be collected by the parent

Staff:

- Staff must have their phones on 'silent' or switched off during class time.
- Staff may not make or receive calls during teaching time. If there are extreme circumstances (eg. acutely sick relative) the member of staff will have made the headteacher aware of this and can have their phone in case of having to receive an emergency call.
- Use of phones must be limited to non-contact time when no children are present.
- Phones must be kept out of sight (e.g. drawer, handbag, pocket) when staff are with children.
- Calls/texts must be made/received in private during non-contact time.
- Phones will never be used to take photographs of children or to store their personal data.
- A school mobile will be carried to sporting fixtures away from school or on an educational visit for contacting parents in the event of an emergency.
- In the event of an unplanned school closure (ie. snow closure or a heating failure) the school mobile will be used to send each family a text message informing them of the change of circumstances. *It is therefore imperative that parents supply school with at least one up-to-date mobile number.*

Parents and other visitors:

- We request that parents do not use mobile phones in the school building or grounds.
- Mobile phones must never be used to take photographs in the school building or grounds.

We very much appreciate our parents' support in implementing this policy in order to keep your children/ our pupils safe.

Appendix 1

Iqra Islamic Primary School
Staff Acceptable Use Policy

School networked resources including SIMS, are intended for educational purposes and may only be used for legal activities consistent with the school's guidelines. If you make a comment about the school or Local Authority you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school or Local Authority into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and /or retrospective investigation of the users use of services and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Condition of Use

Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in the Policy and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network the Leadership Team and the Network Manager.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of guidelines that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the schools ethos and code of conduct.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or county council) into disrepute
2	I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden
3	I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group
4	I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored

5	Privacy – I will not reveal any personal information e.g. home address, telephone number, social networking details; of other users to any unauthorised person. I will not reveal any of my personal information to pupils
6	I will not trespass into other users' files or folders
7	I will ensure that all my login credentials (including passwords) are not shared with any individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users
8	I will ensure that if I think someone has learned my password then I will change it immediately and /or contact the Network Manager and or the Leadership Team
9	I will ensure that I log off or lock my computer, after my network session has finished
10	If I find an unattended machine logged on under other users username I will **not** continue using the machine. I will log off immediately
11	I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the Leadership Team
12	I am aware that email is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the Leadership and possibly the Local Authorities. Anonymous messages are not permitted
13	I will not use the network in any way that would disrupt use of the network by others
14	I will report any accidental access, receipt of inappropriate materials or filtering breaches/unsuitable websites to the Leadership Team and the Network Manager
15	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use
16	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed
17	I will not accept invitations from pupils and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings of images. I will also be careful with who has access to my

	pages through friends and friends of friends. Especially with those connected with my professional duties, such as school, parents and their children
18	I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to, are not confused with my professional role in any way
19	I will only access social networking sites in my own time (once my professional duties are fulfilled) using my own personal mobile devices
20	I will support and promote the school's e-safety and Data Security policies and help pupils be safe and responsible in their use of the Internet and related technologies
21	I will not send or publish material that violates Data Protection Act or breaching the security this act requires for personal data, including data held on SIMS
22	I will not receive, send or publish material that violates copyright law. This includes materials sent/received using Video Conferencing or Web Broadcasting
23	I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system
24	I will ensure that portable ICT equipment such as laptops, digital still and flip cams are securely locked away when they are not being used
25	I will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet will be encrypted or otherwise secured

Network Security

Users are expected to inform the Leadership Team and the Network Manager immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network will be regularly checked by the Network Manager. Users identified as a security risk will be denied access to the network.

Media Publications

Written permission from parents or carers must be obtained before photographs of or named photographs of pupils are published. Examples of pupils work must only be published e.g. photographs, videos, TV presentations, web pages etc. if written parental consent has been given.

Staff User Agreement Form for the Staff Acceptable Use Policy

As a school user of the network resources, I agree to follow the school guidelines (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult with the Leadership Team and or the Network Manager.

I agree to report:

- Any misuse of the network
- Websites that are available on the school Internet that contain inappropriate material
- Any portable equipment e.g. cameras, laptops; that are not in use and not secured to the Leadership Team and Network Manager

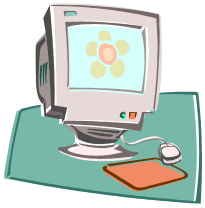
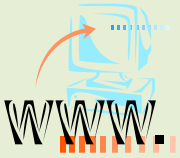
If I do not follow the guidelines, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Staff Name _____
Staff Signature _____
Date _____

Appendix 2

Acceptable Use Policy

Younger Primary Children (Reception, Year1 and 2)

	**I will use school computers for school work and not to upset or be rude to other people**
	I will look after school ICT equipment and tell a teacher straight away if something is broken or not working properly
	I will log off or shut down a computer when I have finished using it
	I will save only school work on the school computer and will check with my teacher before printing
	I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy
	I will only go on websites that my teacher tells me to
	I will tell my teacher straight away if I go on a website by mistake
	I will tell a teacher straight away if I see a website that is not to do with my work

I will read and follow these rules.
I understand that all of my work on school ICT equipment can be seen.
I understand that I must follow these guidelines.

Parent/Carer's signature _____

Child's signature _____
Date _____

Appendix 3

Acceptable Use Policy
Middle Primary Children (Years 3-4)

I will read and follow the rules in the AUP.
I understand that this AUP is regularly reviewed and that there are consequences if I do not follow it.

I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy
I will only use school computers for school work and not to upset or be rude to other people
I will only go on websites that my teacher tells me to
I will tell my teacher straight away if I go on a website by mistake
I will look after school ICT equipment and tell a teacher straight away if something is broken or not working properly
I will not try to download or install any software on school computers
I will only use the username and password I have been given and I will keep them secret
I will save only school work on the school network and will check with my teacher before printing
I will log off or shut down a computer when I have finished using it

I understand that all of my work and internet activity on school ICT equipment can be seen.
I understand that I must follow these guidelines or there will be sanctions and consequences.
Parent/Carer's signature _____

Child's signature _____
Date _____

Appendix 4

Acceptable Use Policy
Older Primary Children (Year 5 & 6)

I will read and follow the rules in the AUP.
I understand that this AUP is regularly reviewed and that there are consequences if I do not follow it.

I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy
I will only use school ICT equipment for my school work and not to upset or bully other people or create a bad impression of my school
I will take responsibility for my own use of all ICT equipment and will use it safely, responsibly and legally e.g. I will make sure that my work does not break copyright
I will not go on any unsuitable or illegal web sites on purpose e.g. rude images, violence and racism. If I go on any by mistake I will tell a teacher straight away
I will tell a teacher if I can see a website that is inappropriate or receive any unwanted emails (such as spam)
I will look after school ICT equipment and report and damage to a teacher straight away
I will not try to get past any security measures in place to protect the school network
I will only use the usernames and passwords I have been given and I will keep them secret
I will save only school work on the school network and will check with my teacher before printing
I will log off or shut down a computer when I have finished using it

I understand that all of my work and internet activity on school ICT equipment can be monitored and that there are consequences if I do not use the equipment sensibly, safely and responsibly

Parent/Carer's signature _____

Child's signature _____
Date_____

Appendix Five