Madani Academy Primary School

e-Safety Policy

Approved/issue	2nd September 2019	**Locations**	Appendix to School Handbook Website School admin staff
Review Cycle	Annual		
Next review due	02nd Septemer 2020	**Circulation details**	Governors All staff Parents via website
CMT responsibility	Headteacher		

Madani Academy Primary School

e-Safety Policy

Definition of Terms

School: Madani Academy Primary School

Headmaster: Headmaster of the School

Pupils, Pupils who attend the School including pupils in the Early Years Foundation
Students: Stage (EYFS)

1 Introduction

1.1 Madani Academy Primary School is a caring community founded upon Islamic values and, as such, the well-being of each of its members is a prime concern.

1.2 Information and Communication Technology (ICT) has transformed the process of teaching and learning in the School. It is a crucial component of every academic subject, and is also taught as a subject in its own right. All Pupils are taught how to research on the internet and to evaluate sources. They are instructed in the importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be treated with caution.

1.3 ICT and the communications revolution provide unrivalled opportunities for enhanced learning, but also pose risks to young people. Pupils are therefore taught how to stay safe in this environment and how to mitigate risk, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.

1.4 When using the Internet to enter or share information it is important that we consider what data we are making available and how this can be viewed by others. Most social networking sites have privacy settings which can and should be used to limit the audience who can access this information.

1.5 The Data Protection Act of 1998 was brought in to protect the rights and privacy of individuals and to ensure that data about them was not processed without their knowledge where possible. It covers data which is held in electronic formats.

It also takes into account the provisions of the General Data Protection Regulation, which is new legislation that came into force in May 2018.

2. Child Protection

2.1 The School recognises that internet safety is a child protection and general safeguarding issue. The Child Protection Lead has been trained in safety issues involved with the misuse of the internet and other mobile electronic devices. They work to promote a culture of responsible use of technology that is consistent with the ethos of the School. All of the staff, especially those with pastoral responsibilities, receive training in e-safety issues.

2.2 The school has a programme on e-safety which ensures that all year groups in the School are educated, in an age-appropriate way, in the risks and reasons why they need to behave responsibly online. The Headmaster is responsible for overseeing the programme.

3. Misuse: Statement of Policy

3.1 The School will not tolerate any illegal material. If it is discovered that a child or young person is at risk as a consequence of online activity, the School may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The School impose a range of sanctions on any Pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-bullying Policy.

4. Involvement with Parents and Guardians

4.1 The School seeks to work closely with parents and guardians in promoting a culture of e-safety. The School will always contact parents/guardians if there are any worries about a child or young person's behaviour in this area, and parents/guardians are encouraged to share any worries with us.

4.2 It is recognised that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home hence the School organises occasions and age-appropriate information evenings for parents/guardians when a specialist offers advice about the potential hazards of this exploding technology, and the practical steps that parents/guardians can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity.

5. ICT Acceptable Use Policy

E-safety is a whole School responsibility, and all staff and Pupils are required to adhere to an ICT Acceptable Use Policy, which incorporates the following guidelines in age appropriate ways:

5.1 Treating Others with Respect

i) The School expects Pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face to face contact. They should always follow the school's Behaviour Code and Regulations, are discussed with pupils and displayed around the schools.

ii) The School expects a degree of formality in communications between staff and Pupils, and would not in normal circumstances expect them to communicate with each other by text or mobile phone.

iii) Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The School is strongly committed to promoting equal opportunities for all, regardless of race, gender, religious affiliation, cultural background, gender orientation or disability.

5.2 Cyberbullying

i) Cyberbullying is a particularly pernicious form of bullying, because it can be pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. The School's Anti-bullying Policy sets out our preventative measures and the procedures that will be followed where we discover cases of bullying.

ii) Proper supervision of Pupils plays an important part in creating a safe ICT environment at school; but everyone needs to learn how to stay safe out with school.

iii) Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to report the matter.

5.3 Keeping the School's Network Safe

i) Certain sites are blocked by the School's filtering system and the system monitors all use of the network and the Headmaster will oversee the checking of this on a regular basis.

ii) The e-mail system used by the School monitors and blocks SPAM and certain attachments.

iii) There is strong anti-virus protection on our network, which has been installed by IT Support.

Acceptable Use Policies for ICT usage are given to all staff and Pupils. The School will impose sanctions for the misuse, or attempted misuse of the internet, mobile phones and other electronic devises.

6. Social Networking Sites and Telephone Communication

6.1 The School staff have a key role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the School system and data and for training our teaching and support staff in the use of ICT. They monitor the use of the internet and e-mails and will report any observed inappropriate usage to the appropriate senior manager. It is the responsibility of all staff to report any inappropriate usage to the IT Manager. Access to sites of inappropriate content is blocked from the School network, as is access to social networking sites such as Facebook during the school day.

6.2 In normal circumstances, staff should not share personal contact details with Pupils and this includes mobile telephone numbers, home telephone numbers, instant messaging identities and social network screen-names. Where this is deemed to be needed for any reason, staff should first discuss the matter with the Headmaster. Staff and Pupils should not have each other as contacts on their personal social networking sites. Staff should not request, or respond to, any personal information from the child/young person other than that which might be appropriate as part of their professional role. If queries exist or if advice is needed, staff should consult, in the first instance, the Headmaster.

6.3 Personal e-mail addresses, instant messaging identities or personal telephones (mobile or fixed line) should never be used to contact Pupils without the explicit agreement of the Headmaster, or, in his absence, his deputy.

6.4 The safest approach is to avoid using personal telephone equipment. Staff and Pupils should use school e-mail and can have access to a school mobile telephone for official business.

7. Video and Photographic Images

7.1 Pupils should not take images (for example, video or photographs) of staff or Pupils without their permission and any images should only be shared with the express permission of those involved.

7.2 Particular issues may arise as a consequence of the ability to create, to store and to manipulate video and photographic images. The safest approach is to avoid using personal equipment and to use a work-provided item for this task. This may not always be possible and the requirements outlined here are aimed at guiding staff and pupils to safe outcomes.

7.3 The Terms and Conditions that parents sign includes a section as follows:

"***Photographs:*** *It is the custom and practice of most independent schools, and of this School, to include some photographs or images of pupils in the School's promotional material. These images may be used in various media, including the School website, social media platforms such as the School's twitter and facebook and YouTube accounts and in the press. We would not disclose the name or home address of a child without the Parents' consent. Parents who do not want their child's photograph or image to appear in any of the School's promotional material must make sure their child knows this and must write immediately to the Head requesting an acknowledgement of their letter.*"

7.4 Staff need to be mindful of the possible child protection issues associated with the possession of images of children and as such they are required to adhere to the following policy.

i) All images and video taken of individual pupils or groups of pupils must be uploaded **as soon as possible** to the School network and then **deleted** immediately from any personal computer, the hard drive of any computer, the memory of any camera or similar device, any personal memory device or other transportable memory.

ii) All images and video of individual pupils or groups of pupils which are delivered to a member of staff as part of their professional work, for example, for an Art display or a marketing initiative, must **not** be stored on any personal computer, the hard drive of any school computer, the memory of any camera or similar device, any personal memory device or other transportable memory and should be uploaded immediately to the School network.

iii) Any manipulation or images or video for any purpose including controlled assessment, coursework, marketing, etc, **must** be undertaken on the School network and the results of that manipulation stored on the network only. Exceptionally, headmaster may have occasion to transmit appropriate video and images to the awarding bodies and will be guided in that by the relevant regulations.

8. Conclusion

ICT has transformed the ways we communicate with others, both in and out of the classroom. Our aim is to promote the positive use of this technology and to discourage inappropriate usage or usage which could put others at risk. Staff are asked to recognise that this policy is designed

above all to protect the interests of the child, to support staff and to ensure that required action is taken as quickly as possible.

Appendix 1 – How Will Infringements be Handled?

Whenever a Pupil or member of staff infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the School management. The following are set out as guidance based on the level of infringement.

1. Students

Category A Infringements

i) Use of non-educational sites during lessons;
ii) Unauthorised use of e-mail;
iii) Unauthorised use of mobile phone (or other new technologies) in lessons, for example, to send texts to friends;
iv) Use of unauthorised instant messaging/social networking sites.

Possible sanctions: referred to class teacher or tutor for a warning and clarification of what can happen if this is repeated / mobile phone removed from pupil and passed to the Assistant Head for collection at the end of the school day

Category B Infringements

i) Continued use of non-educational sites during lessons after being warned;
ii) Continued unauthorised use of e-mail after being warned;
iii) Continued unauthorised use of mobile phone (or other new technologies) in lessons after being warned;
iv) Continued use of unauthorised instant messaging/chatrooms/social networking sites;
v) Use of filesharing software for the purposes of sharing music, games or videos illegally;
vi) Accidentally corrupting or destroying others' data without notifying a member of staff of it;
vii) Accidentally accessing offensive material and/or not notifying a member of staff of it;
viii) Not logging off and/or using another students log on details.

Possible sanctions: referred to class teacher or Headmaster for follow-up action which could include detention or removal of internet and/or e-mail access for a period of time / mobile phone removed from pupil and passed to the headmaster who will contact parents regarding collection of the phone and the length of time when the item cannot be brought into school / referred to the e-Safety Coordinator for a warning of what could happen if this is repeated (particularly for the last two situations)

Category C Infringements

i) Deliberately corrupting or destroying someone's data, violating the privacy of others;
ii) Sending an e-mail or text message that is regarded as harassment or of a bullying nature (one-off);
iii) Deliberately trying to access offensive or pornographic material;
iv) Any purchasing or ordering of items over the internet (without permission from staff);
v) Transmission of commercial or advertising material;
vi) Deliberately using another pupil's login details for malicious purposes and/or passing out your personal login details to another pupil.

Possible sanctions: referred to Headmaster for a warning and clarification of what can happen if this is repeated and contact with parents as well as removal of internet and/or e-mail privileges for a period of time / referred to the e-Safety Coordinator for a warning of what could happen if this is repeated (particularly for the last two situations)/removal of technological device and parent contacted if this is not done via the School network

If inappropriate web material is accessed then ensure the IT Manager is informed and that appropriate technical support filters the site and inform the Headmaster.

Category D Infringements

i) Continued sending of e-mails or text messages regarded as harassment or of a bullying nature after being warned;
ii) Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
iii) Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1998;
iv) Bringing the School name into disrepute;
v) Using the School network as a means of inciting riot or public order offences;
vi) Deliberately trying to circumvent the IT Security Policy.

Possible sanctions: referred to Headmaster, contact with parents which may include exclusion as well as referral to the Community Police / removal of technological device and parent contacted if this is not done via the School network / contact with the Child Exploitation and Online Protection Unit

If appropriate, secure and preserve any evidence, for example, print-outs of e-mails/texts and inform the sender's service provider.

2. Members of Staff

Category A Infringements (Misconduct)

i) Excessive use of Internet for personal activities not related to professional development, for example, online shopping, personal e-mail, instant messaging, etc.;
ii) Use of personal data storage media (for example, USB memory sticks) without considering access and appropriateness of any files stored;
iii) Not implementing appropriate safeguarding procedures;
iv) Any behaviour on the world wide web that compromises the staff members professional standing in the school and community;
v) Misuse of first level data security, for example, wrongful use of passwords;
vi) Breaching copyright or licence, for example, installing unlicensed software on the network.

Possible sanctions: referred to line manager/Headmaster and warning given

Category B Infringements (Gross Misconduct)

i) Serious misuse of, or deliberate damage to, any School computer hardware or software;
ii) Any deliberate attempt to breach data protection or computer security rules;
iii) Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
iv) Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1998;
v) Bringing the school into disrepute.

Possible sanctions: referred to Headmaster/Governors and follow the School's disciplinary procedures; report to Human Resources/involvement of the Police, if appropriate

If there is a safeguarding issue, then remove the PC/laptop to a secure place to ensure that there is no further access to the PC or laptop. If appropriate, instigate an audit of all ICT equipment by an outside agency to ensure there is no risk of pupils accessing inappropriate materials in the School. If appropriate, identify the precise details of the

materials. In the case of indecent images of children including child pornography being found, the member of staff will be immediately suspended and the Police should be called. (The School's Child Protection Policy would be implemented.)