Rochdale Islamic Academy
inspire - believe - achieve
BOYS' SCHOOL

ACCEPTABLE USE OF ICT AND E-SAFETY POLICY

V.1.0

Reviewed: September 2020

Next Review: August 2021

Responsible: Mr Arshad Ashraf

Governing Body Approved: September 2020

Approved: Mr Javaid Kashif (Chair of Governors)

ACCEPTABLE USE OF ICT AND E-SAFETY POLICY

INTRODUCTION

The e-Safety Policy relates to other policies including those for ICT, Acceptable Computer Use, Anti-Bullying and for Safeguarding.

Rochdale Islamic Academy recognises that the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

As part of our commitment to learning and achievement we at Rochdale Islamic Academy want to ensure that the Internet and other digital technologies are used in an Islamic and appropriate manner:

- Raise educational standards and promote pupil achievement.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding.
- To enable this to happen we have taken a whole school approach to E-safety as promoted by British Education Communication Technology Agency (BECTA), which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's ICT infrastructure and technologies.

Rochdale Islamic Academy as part of this policy, holds steadfastly to the Islamic principle of equality that there should be an equitable learning experience for all pupils using ICT technology. We recognise that ICT can allow disabled pupils increased access to the curriculum and other aspects related to learning.

Rochdale Islamic Academy is committed to ensuring that **all** its pupils will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the risks that exist so that they can take an active part in safeguarding children.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, Trustees, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school

premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

The nominated senior person for the implementation of the School's e-Safety policy is Arshad Ashraf.

The policy applies to:

- all pupils;
- all teaching and support staff (including peripatetic), school Trustees and volunteers;
- all aspects of the School's facilities where they are used by voluntary, statutory or community organisations.
-

Rochdale Islamic Academy will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- A range of policies including acceptable use policies that are frequently reviewed and updated;
- information to parents that highlights safe practice for children and young people when using the Internet and other digital technologies;
- adequate training for staff and volunteers;
- adequate supervision of pupils when using the Internet and digital technologies;
- education that is aimed at ensuring safe use of Internet and digital technologies;
- A reporting procedure for abuse and misuse.

REPORTING ABUSE

There will be occasions when either a pupil or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the pupil or adult should report the incident **immediately**.

The School also recognises that there will be occasions where pupils will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances KSCB Procedures should be followed. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Safeguarding within the School will refer details of an incident to the lead agencies involved in safeguarding children, namely Children's Social Care and the Police.

The School, as part of its safeguarding duty and responsibilities will, in accordance with KSCB Procedures assist and provide information and advice in support of child protection enquiries and criminal investigations.

EDUCATION AND TRAINING

Rochdale Islamic Academy recognises that the Internet and other digital technologies can transform learning; help to improve outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience.

As part of achieving this, we want to create within Rochdale Islamic Academy an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely to this end,

Rochdale Islamic Academy will: -

Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum.

Educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem.
Support parents in gaining an appreciation of Internet safety for their children and provide them with relevant information on the policies and procedures that govern the use of Internet and other digital technologies within the school.

COMPUTER VIRUSES

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB stick, CD) must be checked for any viruses using school provided anti-virus software before using them

- Never interfere with any anti-virus software installed on school ICT equipment that you use

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and notify the office immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know

EQUAL OPPORTUNITIES

PUPILS WITH ADDITIONAL NEEDS

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' E-Safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

E-SAFETY

ROLES AND RESPONSIBILITIES

As E-Safety is an important aspect of strategic leadership within the school, the Head and Trustees have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-Safety co-ordinator in this school is Arshad Ashraf who has been designated this role as the headteacher. It is the role of the E-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Rochdale LA, Becta, CEOP (Child Exploitation and Online Protection), Childnet and Prevent.

Senior Leadership and Trustees are updated by the Head/ e-Safety co-ordinator and all Trustees have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, Trustees, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and preventing and protecting pupils from violent extremism.

E-SAFETY IN THE CURRICULUM

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

- The school provides opportunities within a range of curriculum areas to teach about E-Safety

- Pupils are aware of the impact of **Cyberbullying** and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

E-MAIL

Pupils may use e-mail accounts on the school system.

- 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

- E-mail sent by pupils to an external organization should be written carefully and authorized by a member of staff before sending, in the same way as a letter written on school headed paper.

PUBLISHED CONTENT AND THE SCHOOL WEB SITE

- The contact details on the Web site should be the school address, webmaster and school e-mail,

fax and telephone number. Staff or pupils' personal information will not be published.

- The headteacher has overall editorial responsibility and will ensure that content is accurate and appropriate.

PUBLISHING PUPILS' IMAGES AND WORK ON THE SCHOOL WEBSITE

- Photographs that include pupils and any published work will not enable individual pupils to be clearly identified unless permission has been given by parents
- Pupils' names will not be used on the Web site in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

SOCIAL NETWORKING AND PERSONAL PUBLISHING

- The school network technician controls access to social networking, messaging and blogging sites. All have been blocked unless requested by staff and use for educational purpose.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils and parents will be advised that the use of some social network spaces outside school is inappropriate for certain aged groups (11-16yrs)

MANAGING FILTERING

- The network technician controls all internet filtering
- if staff or pupils discover an unsuitable site which is not filtered, it must be reported to the SLT who will inform the network technician
- The School use **opendns** filtering system to manage their computer systems.

INTERNET USE AT HOME

- Parents and carers will be advised that the use of social network spaces outside school is inappropriate and brings a range of dangers for young people.
- Parents are advised not to allow their children unsupervised access to the internet (via posters on parent notice boards)
- Parents will be advised to contact their service provider to explore home filtering and child controls.

E-SAFETY SKILLS DEVELOPMENT FOR STAFF

- Our staff receive regular information and training on E-Safety issues in the form of training by the IT teacher.

- Details of the ongoing staff training programme can be found in the staff training file.

- New staff receive information on the school's acceptable use policy as part of their induction

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community

- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas

MANAGING THE SCHOOL E-SAFETY MESSAGES

- We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used

- The E-Safety policy will be introduced to the pupils at the start of each school year

- E-Safety posters will be prominently displayed

INCIDENT REPORTING, E-SAFETY INCIDENT LOG & INFRINGEMENTS

INCIDENT REPORTING

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's admin staff or E-Safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must also be reported.

E-SAFETY INCIDENT LOG

Some incidents may need to be recorded in other places, particularly is they such as SOLERO, if they relate to a bullying or racist incident. The safety coordinator is responsible for record keeping.

MANAGING THE INTERNET

- The school maintains pupils who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology

- Staff will preview any recommended sites before use

- Raw image searches are discouraged when working with pupils

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research

- The school will block/filter access to social networking sites.

- This protection will be updated regularly by the school technician.

Taking of Images and Film

In order to provide evidence of learning and for promotional purposes and **with the express permission of the Headteacher**, photography and digital images can be taken. In line with the Islamic ethos of the school, photographs and digital images taken in school or offsite must not show the faces of pupils.

Pupils are not permitted to bring into school or to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.

WEBCAMS AND CCTV

- The school uses CCTV for security and safety. The only people with access to this are the headteacher and the office administrative staff.
- We do not use/allow the use of webcams in schoo*l*
- Portable equipment must be transported in its protective case if supplied

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device
- Staff must ensure their phone is switched off on entry into the school premises. Mobile phones must only be used in the staffroom, never in classrooms and never in the presence of pupils.
- Pupils are not allowed to bring personal mobile devices/phones to school.

PUPIL GUIDELINES FOR INTERNET-USE
GENERAL

Pupils are responsible for good behaviour on the Internet, just as they are in a classroom or a school corridor. General school rules apply.

The Internet, primarily, is provided for pupils to conduct research and back-up their work. Parent's/carer's permission is required before a pupil is granted access. Access is a privilege not a right and that access requires responsibility.

Individual users of the Internet are responsible for their behaviour and communications over the network. Users must comply with school standards and honour the agreements they have signed.

Computer storage areas (including any external storage media you bring to school) will be treated like school lockers. Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or storage media are always private.

During school, teachers will guide pupils towards appropriate materials. Outside of school, families bear responsibility for such guidance as they must also exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

The following are not permitted within the school environment:

1. Sending or displaying offensive messages or pictures.
2. Using obscene language.
3. Harassing, insulting or attacking others.
4. Damaging computers, computer systems or computer networks.
5. Violating copyright laws.
6. Using others' passwords or accounts.
7. 'Hacking' into others' folders, work or files for any reason.
8. Intentionally wasting limited resources, including printer ink and paper.

SANCTIONS

1. Violations of the above rules will result in a temporary or permanent ban on internet/computer use.
2. Your parents/carers will be informed.
3. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
4. When applicable, police or local authorities may be involved.
5. If necessary, external agencies such as Social Networking or Email Member sites may be contacted and informed.

PUPILS

- You must have your teacher's permission before using the internet.
- You must have a supervising teacher or member of staff with you at all times when using the internet.
- Do not disclose any password or login name to anyone, other than the persons responsible for running and maintaining the system.
- Do not upload/send personal addresses, telephone/fax numbers or photographs of anyone (staff or pupils) at the school.
- Do not download, use or upload any material which is copyright. Always seek permission from the owner before using any material from the internet. If in doubt do not use the material.
- Under no circumstances should you view, upload or download any material which is likely to be unsuitable for children. This applies to any material of a violent, dangerous or inappropriate context. If you are unsure ask the supervisor.
- Always respect the privacy of files of other users.
- Be polite and appreciate that other users might have different views than your own. The use of strong language, swearing or aggressive behaviour is not allowed. Do not state anything which could be interpreted as libel.
- Ensure that you have followed the correct procedures for using the Internet.

- Report any incident which breaches these rules to your teacher.

Education is essential in helping children and young people to develop their own parameters of acceptable behaviour when online, and allow them to develop their own strategies for protecting themselves when using ICT in situations where the
adult supervision and technological protection offered within the school environment are not available. Children and young people should also be taught to seek help if they experience problems, understanding that they are not accountable, nor should they feel guilty, for the actions of others in which they are unwilling participants. Schools have an important role to play in teaching internet safety. Schools also have an important role to play in helping to educate parents and the wider community.

MONITORING

Monitoring the safe use of the Internet and other digital technologies goes beyond the personal use of the Internet and electronic mail a pupil or member of staff may have. Rochdale Islamic Academy recognises that in order to develop an effective whole school E-safety approach there is a need to monitor patterns and trends of use inside school and outside school (Education and Inspections Act 2006, Section 89(5)).

With regard to monitoring trends, within the school and individual use by school staff and pupils, Rochdale Islamic Academy will audit the use of the Internet and electronic mail in order to ensure compliance with this policy. The monitoring practices of the school are influenced by a range of national and Local Authority guidance documents and will include the monitoring of content and resources.

SANCTIONS

Rochdale Islamic Academy has been careful to develop in conjunction with its partners, policies and procedures to support the innocent in the event of a policy breach and enable the School to manage such situations in, and with, confidence.

Where there is inappropriate or illegal use of the Internet and digital technologies, the following sanctions will be applied:

Child / Young Person

- The child/young person will be disciplined according to the behaviour policy of the school, which could ultimately include the use of Internet and email being withdrawn.
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

Adult (Staff and Volunteers)

- The adult may be subject to the disciplinary process, if it is deemed he has breached the policy
- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

-

If inappropriate material is accessed, users are required to immediately report this to the ICT Department so this can be taken into account for monitoring purposes.

WRITING AND REVIEWING THIS POLICY

STAFF AND PUPIL INVOLVEMENT IN POLICY CREATION

- Staff and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use through the student Shura and school staff meetings

REVIEW PROCEDURE

There will be an on-going opportunity for staff to discuss with the E-Safety coordinator any issue of E-Safety that concerns them

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

This policy will be reviewed every year.

WHAT TO DO IF A CYBER BULLYING INCIDENT OCCURS:

Based on "Cyber bullying – Safe to Learn: Embedding Anti-

bullying work in schools" DCSF00658-2007

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of school time.

1. Advise the child not to respond to the message

2. Refer to relevant policies including e-safety/acceptable use, anti-bullying and PHSE and apply appropriate sanctions

3. Secure and preserve any evidence

4. Inform the sender's e-mail service provider

5. Notify parents of the children involved

6. Consider delivering a parent workshop for the school community

7. Consider informing the police depending on the severity or repetitious nature of offence

8. Inform the School Safeguarding officer/ LA e-safety officer

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform the site administrators and / or ISP and request the comments be removed if the site is administered externally

2. Secure and preserve any evidence

3. Send all the evidence to CEOP (Child Exploitation and Online Protection Centre) at www.ceop.gov.uk/contact_us.html

4. Endeavour to trace the origin and inform police as appropriate

5. Inform School Safeguarding officer/ e-safety officer

The school may wish to consider delivering a parent workshop for the school community

Children and staff should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear, even if they have initially responded to the abuse.