Rochdale Islamic Academy
inspire - believe - achieve
GIRLS' SCHOOL

E-Safety Policy

Reviewed: September 2023

Next Review: September 2024

Approved by Board of Trustees: September 2023

INTENT

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.

Legal Framework

This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997

The policy also has regard to the following statutory guidance:

- DfE Keeping Children Safe in Education 2023

EQUAL OPPORTUNITIES

PUPILS WITH SEND

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. Online activities are differentiated and well managed for these children.

ROLES AND RESPONSIBILITIES

As E-Safety is an important aspect of strategic leadership within the school, the Safeguarding Lead and Trustees have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

It is the role of the IT Manager to keep abreast of current issues and guidance through organisations such as Rochdale Local Authority, CEOP (Child Exploitation and Online Protection), UK Safer Internet Centre, Childnet and Prevent.

The IT Manager alongside the IT Support Company is responsible for ensuring that appropriate filtering and monitoring systems are in place to safeguard pupils. This is to be monitored by the Safeguarding Lead.

The IT Manager alongside the IT Support ensures the network has adequate virus protection and security protocols, e.g., password protection and encryption.

The Safeguarding Lead is responsible for ensuring the day-to-day online safety in the school, and managing any issues that arise.

The Safeguarding Lead will regularly monitor the provision of online safety in the school and will provide feedback to the trustees.

Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and staying safe online is promoted at all times.

All staff are responsible for ensuring they are up to date with current e-safety issues and this policy.

Parents are responsible for ensuring their child understands how to use digital devices and the internet appropriately.

Senior Leadership and Trustees are updated by the IT Manager and all Trustees understand the issues and strategies at our school in relation to local and national guidelines and advice.

This policy is for staff, Trustees, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to and not limited to the following mandatory school policies: Safeguarding, KCSiE, UK GDPR, Home–School Agreements, and Behaviour (including the Anti-Bullying and Cyber-Bullying) policy and preventing and protecting pupils from 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 Computing curriculum.

E-MAIL

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

- Pupils must immediately tell a teacher if they receive an 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 organisation should be written carefully and authorised 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, school e-mail address, telephone number. Staff or pupils' personal information will not be published.
- The IT Manager 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 schools IT support team control 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 IT Support Company, Voktis, control all internet filtering. There is an effective filtering system in place which blocks access harmful sites and inappropriate content.
- The filtering system is applied to:
    - all users, including guest accounts.
    - School owned devices
    - Any device using the school broadband service
- If staff or pupils discover an unsuitable site which is not filtered, it must be reported to the IT Manager/SLT who will inform IT Support.

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 EDUCATION

- Our staff receive regular information and training on E-Safety issues in the form of training by a member of the SLT and online training.
- New staff receive information on the school's Acceptable Use of ICT and E-Safety 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

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 IT Manager/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 if they relate to a bullying or racist incident. IT Manager/SLT are responsible for record keeping.

MANAGING THE INTERNET

- 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 IT support team.

SOCIAL NETWORKING:

- Access to social networking sites will be filtered as appropriate
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times
- Pupils are regularly educated on the implications of posting personal data online, outside of school
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole
- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings
- Staff are not permitted to publish comments about the school which may affect its reputability
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught

IMAGES AND VIDEOS

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 where parental consent has been provided for the students.

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.

CCTV

- The school uses CCTV for security and safety. The only people with access to this are the Trustees, headteacher, SLT and the office administrative staff.
- 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 on silent mode upon entry into the school premises.
- Mobile phones must not be used in the presence of pupils unless the need is approved by the Headteacher in advance.
- Pupils are not allowed to bring personal mobile devices/phones to school unless authorised by the headteacher. Student mobile phone will then be handed in to the admin office at the start of the day and returned to students at the end of the day.

PUPIL GUIDELINES FOR INTERNET USE

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.

SLT 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 always have a supervising teacher or member of staff with you 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 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

All computer activity is monitored, and data may be accessed, and/or investigated as appropriate as part of the school's safeguarding procedures. This is intended to ensure:

- That the security of school equipment and systems are not compromised
- Information retrieval is possible when a user is absent (e.g., due to sickness)
- Crime can be detected and prevented.
- There is no unauthorised use of the IT systems.
- The school implements and supports the 'Prevent' agenda.
- All data that is held and processed in compliance with the Data Protection Act 2018 and the UK GDPR legislation and guidelines.

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/she 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 IT Manager so this can be considered 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 council and school staff meetings.

REVIEW PROCEDURE

There will be an on-going opportunity for staff to discuss with the IT Manager any issues 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:

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 Behaviour, Safeguarding, E-Safety/Acceptable Use of ICT, Anti-Bullying/Cyber Bullying 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 Lead/Safeguarding Deputy/ Local Authority/E-safety Co-ordinator.
9. If malicious or threatening comments are posted on an Internet site about a pupil or member of staff.
10. Inform the site administrators and / or ISP and request the comments be removed if the site is administered externally.
11. Secure and preserve any evidence.
12. Send all the evidence to CEOP (Child Exploitation and Online Protection Centre) at www.ceop.gov.uk/contact_us.html
13. Endeavour to trace the origin and inform police as appropriate.

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.

Any concerns or complaints relating to staff misuse should be immediately reported to the headteacher. A chosen senior leadership team member or the IT Manager will investigate alleged violations of this policy with the assistance of the IT support team as necessary. According to professional expectations and standards, this might result in disciplinary action and, in severe instances, could result in dismissal.