AL-SADIQ SCHOOL

e-SAFETY POLICY

To be read in conjunction with

SAFEGUARDING CHILDREN AND CHILD PROTECTION POLICY

2024/25

School:	Al-Sadiq School
Head Teacher:	Mr S A Khoei

Named Personnel with designated responsibility for Child Protection (Child Protection Team)	
Designated Safeguarding Lead:	Mrs S Rizvi
Deputy Safeguarding Lead:	Mr. M Al-Bayati & Mrs Z Aldabagh (SLT) (KS3 and KS4), Mrs E Jaffri (KS1 and KS2))
ICT Support Services & e-Safety Coordinator	Mr. M Al-Bayati

Policy Review Dates	
Academic year:	2024/25
Review Cycle:	Annual
Last Review Date:	4th OCTOBER 2024
Al-Khoei Foundation Ratification:	
Date Shared with Staff:	
Next Review Date:	5th SEPTEMBER 2025

Linked Policies:	• AZ SAFEGUARDING POLICY 24-25 • AZ ANTI-BULLYING POLICY 24-25 • AZ EXTREMISM AND PREVENT POLICY 24-25 • AZ BEHAVIOUR POLICY 24-25 • AZ CHILD-ON-CHILD ABUSE POLICY 24-25 • AZ DATA PTOTECTION 24-25 • AZ LOW LEVEL CONCERNS 24-25 • KCSIE 2024

TABLE OF CONTENTS

1. INTRODUCTION

The Proprietors of Al-Sadiq school recognise that the internet and other digital technologies provide a vast opportunity for children and young people to learn. Unlike any other mode of technology, 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.

Al-Sadiq school holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using digital technology. We at Al-Sadiq school are committed to ensuring that all its pupils will be able to use existing, as well as upcoming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents/ carers, are educated as to the dangers that exist so that they can take an active part in safeguarding them.

i. Policy Aims

As part of our commitment to learning and achievement Al-Sadiq school aims to:

- Ensure that pupils benefit from all learning opportunities offered by the internet resources provided by the school in a safe and controlled manner.
- Ensure that all staff benefit from internet access, with clear guidance on safe and acceptable use.
- Provide guidance to staff and pupils about the acceptable use internet and other digital technologies, both the school's and personal items that are brought into either school or outside.

ii. Preventative Work

As part of our recognition of the dangers of internet and other digital technologies, we at Al-Sadiq school have allocated curriculum time to teach pupils about online safety more generally. Pupils are taught about safeguarding, including e-safety, through teaching and learning opportunities, as part of providing a broad and balanced curriculum. This includes covering relevant issues through personal, social, and health education (PSHE), Computer Science lessons, other related subjects, and in our whole school assembly programme. Moreover, students are thought to be critically aware of the materials / content they access on-line or otherwise and be guided to validate the accuracy of information.

Moreover, as it is essential that children are safeguarded from potentially harmful and inappropriate online material, the proprietors of Al-Sadiq school

have also taken steps to ensure appropriate filters and appropriate monitoring systems are in place. Whilst it is essential, and we have ensured that appropriate filters and monitoring systems are in place; the proprietors of Al-Sadiq school believe that over blocking does not lead to unreasonable restrictions as to what children can be taught with regards to on-line teaching and safeguarding.

The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the Al-Sadiq school Safeguarding Children and Child Protection policy. Additionally, this e-Safety policy will help to ensure the safe and appropriate use these new technologies which may potentially put our pupils at risk within and outside the school.

iii. Key e-Safety Messages

It is important that all staff are aware of the key risks and safety messages for children and parents/ carers in order to use the internet safely so that they can advise children and parents/ carers accordingly.

Children need to be guided on:

- the benefits and risks of using the internet;
- how their behaviour can put themselves and others at risk;
- what strategies they can use to keep themselves safe;
- what to do if they are concerned about something they have seen or received via the internet;
- who to contact to report concerns;
- that they won't be blamed if they report any e-safety incidents;
- that cyber bullying cannot be tolerated;
- the basic principles of "netiquette" (how to behave on the internet).

Staff should be aware that some children may be more vulnerable to risk from internet use, generally those children with a high level of computer skills but coupled with poor social skills.

iv. Safe Use of Digital Devices (within and outside the School)

- When using the internet and internet search engines, children should receive the appropriate level of supervision for their age and understanding. Search engines should have an appropriate level of filtering to block access to unsuitable sites;

- When using email and posting message of MS Teams, children should be taught:
    - to keep messages polite,
    - not to disclose personal contact details for themselves or others,
    - to tell their parent or carer immediately if they receive an offensive, or distressing email,
    - not to use these platforms to bully or harass others,
    - be wary of opening attachments where they are unsure of the content or have no knowledge of the sender.

- Pupils are unable to access social media accounts, such as Facebook or Twitter, at school. We recognise that young people have access to unfiltered internet when using smartphones; our strict no-smartphone policy ensures that these are not accessed within the school environment. Random checks are conducted to ensure pupils are complying with this rule. Staff should remind parents and carers to stay vigilant when pupils are using their phones outside school. Although children may bring a basic mobile phone, it must remain switched off during school hours. To further support this policy, students are provided with secure smart phone lockers, allowing them to store their phones safely in the morning and collect them on their way home.

- Children should be taught if using social networking sites such as newsgroups and forum sites:
    - not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended,
    - not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted,
    - how to set up security and privacy settings on sites to block unwanted communications or deny access to those unknown to them,
    - to behave responsibly whilst on-line and keep communications polite,
    - not to respond to any hurtful or distressing messages but to let their parents/ carers know so that appropriate action can be taken.

- Children should be taught not to use chat rooms particularly since many do not have registration or are not age appropriate. In any case they should not give out personal details to anyone on-line that may help to identify or locate them or anyone else. They should not arrange to meet anyone whom they have only met on-line, and let their parents/ carers

know so that appropriate action can be taken. Parents and children should be made aware that bullying or harassment via chat rooms or instant messaging may have serious consequences.

- When using cameras in digital devices, children should be taught:
  - to use them only with people who are well known to them,
  - not to do anything that makes them feel uncomfortable or embarrassed,
  - to tell their parents/ carers if anyone is trying to force them to do something they don't want to.

Staff should be aware that children with learning difficulties may be more vulnerable to risk from use of the internet and may need additional guidance on e-safety practice as well as closer supervision. Staff may wish to discuss this with parents/ carers and help them to access information and resources from specialist agencies.

v. Monitoring and filtering

Filtering and monitoring are two distinct, yet interconnected measures employed to ensure the safety and security of pupils within the digital landscape. Filtering refers to the systematic process of screening and controlling access to online content, aiming to prevent pupils from encountering inappropriate, harmful, or age-inappropriate material. On the other hand, monitoring involves the continuous observation and oversight of pupils' online activities, allowing educators and administrators to promptly address any concerning behaviours or breaches of digital conduct.

We employ a filtering software known as "Classroom Spy," which plays a pivotal role in our efforts to maintain a secure digital environment. This software not only blocks access to inappropriate websites but also offers the ability to filter content based on specific words, phrases, and content types. This comprehensive approach ensures that our pupils are shielded from encountering any content that may pose risks to their safety or disrupt their learning experience.

Within our school organisation, we use the online platforms "MS Teams". This platform is set so any external access is restricted, ensuring that our pupils engage with this platform exclusively within our secure educational environment. This measure further bolsters our commitment to online safety.

In addition to these controls, we have taken steps to disable private chat functionalities within "MS Teams". This means that pupils cannot engage in private conversations with each other or their teachers, promoting transparency and minimising the potential for inappropriate interactions.

Furthermore, we have restricted the features of message deletion or editing within "MS Teams." This restriction ensures that communication remains accountable, discouraging any attempts to alter or erase messages.

Our dedication to fostering responsible digital citizenship goes beyond filtering and monitoring. Our school curriculum is thoughtfully enriched with the aim of raising awareness about best practices when using the internet. Subjects like Computer Science and PSCHE provide pupils with a curriculum that not only enhances their knowledge but also instils the principles of good digital citizenship. Through these subjects, pupils develop the skills and understanding necessary to navigate the online world safely and responsibly.

Simultaneously, our monitoring efforts play a crucial role in maintaining student safety. Through dedicated monitoring software, we can track pupils' online activities, identifying any signs of cyberbullying, inappropriate communication, or potential exposure to harmful content. These monitoring mechanisms are not intended to invade pupils' privacy but rather to intervene when their well-being is at risk, fostering a culture of responsible digital citizenship.

The software "Classroom Spy" also plays a crucial role in monitoring our pupils' online activities when they access computers within the school premises. This software enables educators and administrators to observe and oversee pupils' digital interactions in real-time, ensuring that they are using school resources responsibly and in accordance with our established guidelines. This proactive monitoring not only allows us to address any potential issues promptly but also reinforces our commitment to maintaining a secure and conducive digital learning environment.

As a school committed to providing a safe and enriching learning environment, we are dedicated to staying abreast of the latest advancements in filtering and monitoring technology. By doing so, we ensure that our child protection policies remain effective and relevant, safeguarding our pupils as they navigate the vast online realm.

vi. Published Content and the School Website

- The contact details on the website should be of 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;
- The Head Teacher appointed website coordinator will have a day to day responsibility for Al-Sadiq school website;
- Al-Sadiq school policies including the e-Safety Policy, Safeguarding Children and Child Protection Policy and other useful preventative information would be placed for students, parents/ carers to benefit.
- If a photograph is published, then a name of the child will not be used. Parents/ Carers will sign a permission form when their child enters either school to agree or refuse permission for their child’s work/ photo to

appear on the website from time to time. The paper copy will be kept in the child's file.

2. DEALING WITH SPECIFIC RISKS

i. Cyber Bullying

Cyber bullying is defined as the use of IT to deliberately hurt or upset someone. Unlike traditional physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience. Cyber bullying is extremely prevalent as children who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous. In extreme cases, cyber bullying could be a criminal offence.

Bullying may take the form of:

- Rude, abusive or threatening messages via email or text,
- Posting insulting, derogatory or defamatory statements on blogs or social networking sites,
- Setting up websites that specifically target the victim,
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or email (for example, "happy slapping").

Most incidents of cyber bullying will not necessarily reach significant harm thresholds and will probably be best dealt within the anti-bullying policy structure with the co-operation of parents/ carers. Moreover, children should be taught:

- not to disclose their password to anyone,
- to only give out mobile phone numbers and email addresses to people they trust,
- not to disclose their personal information on social networking pages,
- to only allow close friends whom they trust to have access to any social networking page used,
- not to respond to offensive messages,
- to tell their parents/ carers about any incidents immediately.

Parents/ Carers should be taught to be vigilant about possible cyber bullying and how to work with internet and mobile service providers to cut down on the risk of cyber bullying. They should be made aware that:

- mobile phone companies can trace calls and ensure that any further calls and texts from that number are blocked,
- internet service providers can trace messages being sent from a personal email account and can block further emails from the sender,

- children should not use chat rooms and if used and bullying takes place, the child should leave the chat room immediately and seek advice from parents/ carers; this should be reported to any chat room moderator to take action,
- website providers can remove comments from social networking sites and blogs and in extreme cases, can block the bully's access to the site,
- the child could potentially change their mobile phone numbers or email address.

Where cases of cyber bullying involve significant harm to the victim, advice should be taken from Brent Local Authority Designated Officer (LADO), and/or reported to them or the police. These will be incidents where the bullying is, for example:

- Extreme, for example, threats against someone's life,
- Involves sexual bullying or harassment,
- Continues over a period of time,
- Involves several perpetrators or may be gang related,
- Has a considerable impact on the victim.

ii. Inappropriate Contacts and Non-Contact Sexual Abuse

Concerns may be raised about a child being at risk of sexual abuse as a consequence of their contact with an adult they have met over the internet. Children and parents/ carers should be advised how to terminate the contact and change contact details where necessary to ensure no further contact. Parents/ Carers should be advised to be vigilant of their child's internet use and report any concerns or incidents.

Children may also be sexually abused on-line through video messaging such as WhatsApp, FaceTime and Snapchat. In these cases, perpetrators persuade the child concerned to carry out sexual acts while the perpetrator watches/records. The perpetrators may be adults but may also be peers. In the event of an incident, the child should be taught how to use the Child Exploitation and Online Protection Centre (CEOP) which works across the UK tackling child sex abuse and providing advice for parents/ carers and contact the police to report the incident.

All staff must report suspected cases immediately to the Core safeguarding leads (or Deputy) / Child Protection Team who will respond to cases and if necessary refer and liaise with the LADO, the Police and other agencies to safeguard pupils.

iii. On-line Child Sexual Exploitation

Child Sexual Exploitation (CSE) involves exploitative situations, contexts and relationships where young people receive something (for example food, accommodation, drugs, alcohol, gifts, money or in some cases simply affection) as a result of engaging in sexual activities. Sexual exploitation can take many forms ranging from the seemingly “consensual” relationship where sex is exchanged for affection or gifts, to serious organised crime by gangs and groups. Staff should be aware that children can be sexually exploited on-line, for example posting explicit images of themselves in exchange for money or goods. If staff are concerned that a child they work with is being sexually exploited on-line, they should report suspected cases immediately to the Core safeguarding leads (or Deputy) / Child Protection Team who will respond to cases and if necessary refer and liaise with LADO, the Police and other agencies to safeguard pupils.

iv. Contact with Violent Extremists

Protecting children from the risk of radicalisation should be seen as part of schools’ wider safeguarding duties as indicated by Al-Sadiq school Preventing Extremism and Radicalisation Policy, and is similar in nature to protecting children from other forms of harm and abuse. During the process of radicalisation, it is possible to intervene to prevent vulnerable people being radicalised. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism.

The internet and the use of social media in particular has become a major factor in the radicalisation of young people. As with managing other safeguarding risks, Al-Sadiq school staff should be alert to changes in children’s behaviour which could indicate that they may be in need of help or protection. Al-Sadiq school staff should use their professional judgement in identifying children who might be at risk of radicalisation and act proportionately which may include making a referral to the Channel programme.

The Department for Education has also published advice for school on the Prevent duty. The advice is intended to complement the Prevent guidance and signposts other sources of advice and support.

Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

- All staff need to be aware of those young people who are being targeted by or exposed to harmful influences from violent extremists via the

internet. Young people should be warned of the risks of becoming involved in such groups and it should be against service policy to access such sites;

- The filtering systems used by Al-Sadiq school blocks inappropriate content, which includes extremist content but staff need be vigilant. No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in Safeguarding Children and Child Protection policy;

- A review of filtering should taking place if and whenever there is any incident of a young person accessing websites advocating violent extremism. Where staff, pupils find unblocked extremists content they must report this to the e-safety coordinators/ Child Protection Team/ Head Teacher immediately;

- The e-safety coordinator records and reviews all incidents in order to establish whether there are any patterns of extremist groups targeting the service an e-safety incident report is sent to LADO;

- If there is evidence that a young person is becoming deeply enmeshed in the extremist narrative, or there is evidence that their parents/ carers are involved in advocating extremist violence, the Core safeguarding leads (or Deputy) will make referrals to appropriate agencies with regards to concerns about radicalisation, liaise with partners, including LADO and the police, access programmes under the Channel project to prevent radicalisation and report to the Head Teacher on these matters.

v. Websites Advocating Dangerous Behaviours

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance or alcohol abuse. Exposure to potentially harmful materials on-line may normalise the issue for young people and desensitise them to the harm. Although most people who visit these sites will not be adversely affected, but vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

Al-Sadiq school provide young people with an opportunity to discuss issues such as self-harming and suicide in an open manner and support any young person who is affected by these issues. Staff should be aware of these issues so that they are able to identify those young people who are at risk, and offer appropriate support and make appropriate referrals for help. Where staff are

aware that a young person is accessing such websites, they should make a referral to the Core safeguarding leads (or Deputy) / Child Protection Team who will respond to cases and if necessary refer and liaise with LADO.

3. RESPONSIBILITIES

The Proprietors of Al-Sadiq school recognise that child protection and safeguarding includes e-Safety and that this is paramount to the pupils' welfare. Al-Sadiq school have a special Child Protection Team wherein specific roles are allotted to members who deal with child protection issues and will the Core Safeguarding Leads will act as e-safety coordinators. Al-Sadiq school will ensure that those members of the Child Protection Team undergo updated child protection training every two years. Moreover, The Head Teacher will ensure that there is a system in place to allow for monitoring and support for the e-safety coordinators in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

All our staff must maintain an attitude of "it can happen here" when safeguarding is concerned. By being alert, questioning behaviour, and seeking help from the Child Protection Team when worried about the welfare of the child including e-Safety issues. Staff members should always act in the interest of the child and report any concerns as per Al-Sadiq school procedures as set out in our Safeguarding Children and Child Protection Policy.

i. E-Safety Coordinator:

The e-Safety Coordinator takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.

- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Provides training and advice for staff;
- Liaises with Schools ICT Support Services;
- Receives reports of e-safety incidents and ensures a log of incidents to inform e-safety is kept by the ICT Support Services;
- Reports regularly to the Child Protection Team;
- Liaises with the Head Teacher.

ii. E-Safety Safeguard:

The E-Safety Safeguard is a member of the safeguarding team with specific knowledge and experience in handling cases that involve technology abuse.

This role is crucial in addressing incidents such as cyberbullying, online grooming, and inappropriate internet use by students or staff.

- Investigates and manages safeguarding cases involving technology abuse;
- Coordinates with the e-Safety Coordinator and other safeguarding staff to support comprehensive e-safety practices;
- Provides specialised support to students and staff on e-safety matters related to technology misuse;
- Offers guidance on appropriate actions and helps establish a safer digital environment in the school.

iii. ICT Support Services

Al-Sadiq school ICT Support staff would be responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
- It meets the e-safety technical requirements outlined in this document;
- That users may only access the school's networks through a properly enforced password protection arrangement;
- The Internet Service Provider is informed of issues relating to filtering;
- School's filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant;
- School ICT systems capacity and security will be reviewed regularly;
- That the use of the network/ remote access / email/ school portal is regularly monitored in order that any misuse / attempted misuse can be reported to the e-Safety coordinator for investigation/ action / sanction;
- That monitoring software / systems are implemented and updated as agreed by the e-safety coordinator and the Head Teacher.

iv. Teaching and Support Staff

All Al-Sadiq school members of staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices, which they have read, understood;
- They report any suspected misuse or problem to the Core Safeguarding Leads,

- Digital communications with students should be on a professional level and only carried out using official school emails, school portal or the school phone and not with personal mobiles or e-mails;
- E-safety issues are embedded in all aspects of the curriculum and activities;
- Students understand and follow Al-Sadiq school e-safety and acceptable use policy, which can be accessed on school website;
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor ICT activity in lessons, extra-curricular and extended school activities;
- They are aware of the strict student no smart mobile phone policy within our school, and that they monitor that the policy is implement;
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use;
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data;
- Memory sticks / cards and other mobile devices which cannot be password protected, can only be used on devices with approved virus and malware checking software the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete;
- When using cloud based storage, it is also necessary that staff ensure that only appropriate and authorised parties have shared access;
- All computers are secured with password to access the intranet and World Wide Web through school computers. Staff are responsible for the use of computers while in their possession and should therefore be careful about who has access to their password.

Staff must not use their mobile phone as a camera in Al-Sadiq school. Any photograph/video must be taken using school’s equipment and staff must only save images taken on Al-Sadiq school computers. The recording, taking and sharing of images, video and audio on any mobile phone must be avoided; except where it has been explicitly agreed otherwise by the Head Teacher. Such authorised use is to be monitored and recorded. The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote extremism, pornography, violence or bullying. Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets as these are designated “mobile use free” areas. The Bluetooth or similar function

of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

v. Child Protection Team

The Child Protection Team has the key responsibility for investigating e-safety incidents where the child is thought to be at risk of suffering significant harm. Incidents where an e-safety incident raises child protection concerns will be investigated via child protection procedures. The Child Protection Team will also investigate e-safety incidents that involve inappropriate internet use by members of staff, as this raises concerns about the person's continued fitness to work with children and such confirmed incidents are reported to the LADO. Al-Sadiq school understand that 'Accountability and Integration' require close knitted relationships between the Child Protection Team and LADO, NHS, Social Services and the Police.

Child Protection Team responds to the continually changing challenges by regularly attending appropriate child protection training programmes hosted by the Local Authority and other agencies and also issues regular safeguarding bulletins which is emailed to all staff through Al-Sadiq school internal email system.

vi. The Head Teacher

- The Head Teacher is responsible for ensuring the safety (including e-safety) of members of the school community, although the day to day responsibility for e-safety is delegated to the e-Safety coordinator and the ICT support services;
- The Head Teacher is responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant;
- The Head Teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles;
- The Child Protection Team will address child on child allegations with the Head Teacher involvement, but the Head Teacher will address staff allegations with the involvement of the Proprietors, and allegations made against the Head Teacher must be notified to the Proprietors, LADO and other agencies directly.

vii. Students (and Parents/ Carers)

All Al-Sadiq school students (and parents/ carers):

- Are responsible for using the ICT systems in accordance with the Al-Sadiq school policy;
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Will be expected to know and understand e-safety issues related to the mobile devices, Al-Sadiq school strict no mobile phone policy;
- They should also know and understand school policies on the taking / use of images, cyber-bullying, sexting, initial ceremonies and gang activities;
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the e-Safety Policy covers their actions out of school, if related to their membership of the school.

In particular, parents/ Carers should be alert to the need for vigilance when pupils are using their phones outside the school and that appropriate action can be taken that bullying or harassment via chat rooms or instant messaging may have serious consequences. Importantly, if their child is about to meet an adult they have made contact with on the internet or their mobile phones, they should contact the police on 999 immediately. Parents/ Carers can contact LADO for advice on making a referral where there are concerns that the child:

- is being groomed for sexual abuse,
- is planning or has arranged to meet with someone they have met online,
- has already been involved in making or viewing abusive images,
- has been the victim of non-contact sexual abuse,
- has an interest to sites advocating dangerous activities such as self-harming, suicide or anorexia,
- is being radicalised through internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts.

Annex A; Responsible Internet Use

i. Rules for Staff and Students at School

- The following responsible Internet Use statement helps to protect students, staff and the school by clearly stating what use of computer resources is acceptable and what is not.
- Irresponsible use may result in the loss of Internet access, in line with the School's Behaviour Policy.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's education or to staff professional activity.
- Copyright and intellectual property rights must be respected. E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Users are responsible for e-mail they send and for contacts made.
- The use of social networking sites (Facebook, etc.) are not permitted on site by students.
- Anonymous messages and chain letters are not permitted.
- The use of unauthorised chat rooms is not allowed.
- The school ICT systems may not be used for private purposes, unless the Head teacher has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is not permitted. ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.
- The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

ii. Letter for Parents/ Carers

Dear Parents/Carers

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, Al-Sadiq school is providing access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and an essential skill for all students as they grow up in the modern world. Please could you read the attached - Rules for Responsible Internet Use and sign and return the consent form so that your child may use the Internet at school. If you wish to see a full copy of the school's 'E-Safety and Acceptable Use Policy' this can be emailed to you upon request.

Although there are concerns about students potentially having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.

Yours sincerely

Mrs Z Rizvi

Head Teacher

iii. Consent Form ICT Use & Access

Responsible Internet Use

Please complete, sign and return to your child's form Tutor or Class Teacher I have read, and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times for the duration that I am registered at Al-Sadiq school.

Student's Agreement

Signed: _____ 2024/25

Please print name:

_____

I have read and understood the school rules for responsible Internet use and give permission for my son / daughter to access the Internet for the duration they are registered at Al-Sadiq school. I understand that the school will take all reasonable precautions to ensure students cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Parent's Consent for Internet Access

Signed: _____ 2024/25

Please print name:

_____

Parent's Consent for Web Publication of their child's Work

YES / NO (please circle)

If NO: Please explain to your child, the STUDENT must be responsible to tell the teacher/member of staff if a situation occurs where their photograph is likely to be taken they must state this at the time.

Signed: _____. 2024/25

iv. Staff Declaration

Al-Sadiq school Staff ICT /E Safety

If you have use of school computer equipment or Tablet at home or work signing this declaration implies full understanding of the School ICT /E-Safety Policy as described in the school E-Safety policy

I (Print in block capitals)
.....
declare that:

- Any computer equipment loaned to me from school to use at home or school is to be used solely by me for the purposes of my profession, any personal use is minimal and insignificant. No personal gain will be sought, Personal use in school is also extremely rare.
- Any programs/software/technology/telephones/email use sourced from Al-Sadiq school remains the property of the school and will be used within set boundaries.
- Access codes and personal passwords will remain confidential to the owner. If you bring (use) your own device – there are specific rules regarding security of school data and software. I am fully aware of these rules.
- I understand records kept will be for inspection if required. Checks of accounts would take place by school management both randomly and/or if there are any suspicions that a person's actions may be a threat to the integrity of the school, staff disciplinary concerns or to E-Safety. These could happen at any time, authorised by the Head Teacher, who is advised by the LEA and Police.
- I have read and understood the school policy (available on the shared drive), Breach of this Policy could have serious disciplinary consequences up to and including dismissal.
- I fully understand and agree to abide by the set procedures and will ask if unsure.

Signed: 2024/24

Please print name:

_____