E-Safety Policy

Contents

Policy Statement

Background

Lady Aisha Academy recognises that Information Technology, (IT) and the internet are excellent tools for learning, communication and collaboration. These are accessible within the school for enhancing the curriculum, to challenge pupils, and to support creativity and independence. Using IT to interact socially and share ideas can benefit everyone in the school community. However, it is important that the use of IT and the internet is understood and that it is the responsibility of pupils, staff and parents, to use it appropriately and practise good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Scope

E-safety does not just cover the internet and available resources, but all different types of devices and platforms (e.g. smartphones devices, wearable technology and other electronic communication technologies). Lady Aisha Academy understands that some adults and young people will use these technologies to harm children, thus the school has a 'duty of care' towards any staff, pupils or members of the wider school community, to educate them on the risks and responsibilities of e-safety. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy governs all individuals who are given access to the school's IT systems.

Purpose

This policy aims to be an aid in regulating IT activity in the school, and provide a good understanding of appropriate IT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through Lady Aisha Academy's anti-bullying policy and procedures.

If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the school's child protection procedures (see the school's safeguarding and child protection policy).

Mandate

Roles and responsibility

The head teacher and Designated Safeguarding Lead (Mr Naeem Aslam), the deputy head teacher (Ms Rabiba Khanom), the e-safety Lead (Ms Reha Ullah) and the deputy DSLs (Mrs Aslam and Ms Nafeesa Mistry) will ensure that the e-safety policy is implemented and that compliance with the policy is monitored. The day-to-day management of e-safety in the school is the responsibility of the e-safety Lead (Ms Reha Ullah). She will work closely with the Head of PSHE (Ms Malak Elsouri) and senior pastoral and academic staff in this regard.

Mr Aslam will undertake an annual review of the school's safeguarding procedures and their implementation, which will include consideration of how pupils may be taught about safeguarding, including online safety, through the school's curricular provision, ensuring relevance, breadth and progression.

The head teacher is also responsible for the security of the school's technical infrastructure and filtering systems. At present this is managed by AM Networking in the following ways:

- Internet use is filtered through the software Untangle
- AM Networking keep fortnightly back-ups of school data
- Appropriate restrictions/file permissions for students/staff/school administration

Communicating school policy

All individuals issued access to the school's IT will be provided with a copy of the E-safety policy and this policy is available for all to access, when and as they wish, from the school office. The policy is also published on the school website, for anyone to access. Rules relating to the School Code of Conduct when online, and e-safety guidelines, are displayed around the school and in the computer room. E-safety is integrated into the curriculum in any circumstance where the internet or technology is being used, as well as being specifically addressed in the Computing and PSHE curriculum.

Making use of IT and the internet in school

Using IT and the internet in school brings many benefits to pupils, staff and parents. The internet is used to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a large part of everyday life, education and business. Lady Aisha Academy endeavours to equip pupils with all the necessary IT skills for them to progress confidently between the key stages, into further education, or into a professional working environment once they leave school.

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils, (some age specific). Lady Aisha Academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee

that unsuitable material will never appear on a school computer or device connected to the school network. The school cannot accept liability for the material accessed, or any consequences of internet access unless found to be negligent.

Expectations of use of school computers apply to staff and pupils both in and out of lessons.

Learning to evaluate internet content

With so much information available online, it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Pupils will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate, (e.g. “fake news”);
- about the risks associated with using the internet and social media apps or sites and how to protect themselves and their peers from potential risks;
- how to recognise suspicious, bullying or extremist behaviour;
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- the consequences of negative online behaviour; and
- how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the school will deal with those who behave badly.
- Serious incidents of cyberbullying or malicious communication may need to be referred to the police for further investigation or where a criminal infringement is suspected.
- The school will endeavour to treat all parties with consideration and discuss the implications of their behaviour as part of their development as young people.

The school provides e-safety guidance to staff to better protect pupils and themselves from online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development training includes training on online safety together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles within the organisation, legal changes and requirements.

If staff or pupils discover unsuitable sites then the URL, time, date and content must be reported to any member of staff. Staff need to log this and report it immediately to the website search engine provider. E.g. Google. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies via the head teacher or senior member of staff. Regular checks will take place to ensure that filtering services and e-safety processes are in place, functional and effective.

Managing information systems

The school is responsible for reviewing and managing the security of the IT services and networks that it operates and takes the protection of school data and personal protection of the school community seriously. This means protecting the school network, (as far as is practicably possible), against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by the IT Support team and other third parties engaged with the school. Anti-Virus and Malware protection software will be updated regularly. Some safeguards that the school takes to secure computer systems are:

- Making sure that unapproved software is not downloaded or installed to any school computers. Downloading and changing software on the school computers is password protected, and the password is only accessible by office staff, management staff, and the IT support team.

- The use of user logins and passwords to access the school network are enforced and unique. Office personnel have access to each student's account and can reset passwords at any time

- Portable media containing school data or programmes will not be taken off-site without specific permission from the head teacher.

For more information on data protection in the school, please refer to the school's Data Protection Policy, which can be accessed from the school office. More information on protecting personal data can be found in section 2.11 of this policy.

Emails

Lady Aisha Academy uses email internally for staff and pupils, and externally for contacting parents, and conducting day to day school business and is an essential part of school communication. The school has the right to monitor emails, attachments and their contents but will only do so if there is suspicion of inappropriate use.

School email accounts and appropriate use

Staff should be aware of the following when using email in school:

- Staff should use their school email accounts for school-related matters, contact with other professionals for work purposes and to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people.

- Emails sent from school email accounts should be professional and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.

- The school permits the incidental use of staff school email accounts to send personal emails if such use is kept to a minimum and takes place substantially out of normal working hours. The content should not include or refer to anything which is in direct competition to the aims and objectives of the school nor should it include or refer to anything which may bring the school into disrepute. Personal emails should be labelled 'personal' in the subject header. Personal use is a privilege and not a right. If the school discovers that any member of staff has breached these requirements, disciplinary action may be taken.

- For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by a senior member of staff.
- Staff must tell a member of the senior management team if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

- The forwarding of chain messages is not permitted in school.

Pupils should be aware of the following when using email in school:

Pupils will be taught to follow these guidelines through the IT curriculum and in any instance where email is being used within the curriculum or in class:

- All pupils are provided with a school email account and pupils may only use approved email accounts on the school system during school hours.

- Pupils are warned not to reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission. Excessive social emailing can interfere with learning and in these cases, will be restricted.

- Pupils should immediately inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

Published content and the school website

The school website is viewed as a useful tool for communicating the school ethos and practice to the wider community. It is also a valuable resource for prospective parents and pupils, current parents, pupils and staff for keeping up-to-date with school news and events, celebrating whole-school achievements, personal achievements and promoting the school.

The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and transparency policies.

Office staff are responsible for publishing and maintaining the content of the school website.

They should take care not publish anything on the internet that might bring the school into disrepute. Any pupil or member of staff is welcome to discuss material with the deputy head or the head teacher.

Policy and guidance of safe use of children's photographs and work

Colour photographs and pupils' work bring the school to life, showcase pupils' talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Images of pupils and staff are only displayed in the newsletter and on the website. Consent is obtained from the parents or the pupil themselves, and this depends upon the maturity of the pupil. All parents are asked to tick a box giving consent / withholding consent for their child to be photographed when signing the Pupil Agreement during their child's registration.

Using photographs of individual children

Children may not be approached or photographed while in school or doing school activities without the school's permission, except for parents taking photographs or videos at school events involving their son or daughter for personal use only.

The School follows general rules on the use of photographs and videos of individual children:

- Electronic and paper images will be stored securely.
- Staff will only use equipment provided or authorised by the school, **(not their own device).**
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed.
- For public documents, including in newspapers, full names will not be published alongside images of the child without the consent of the parents or the child (as appropriate). Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the pupils such as school drama productions or sports events must be used for personal use only.
- Pupils are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification always, and will not have unsupervised access to the pupils.

Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to the complaints procedure for more information on the steps to take when raising a concern or making a complaint. Any issues or sanctions will be dealt with in line with this policy.

Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bullet-in boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that the school educates pupils so that they can make their own informed decisions and take responsibility for their conduct online. Lady Aisha Academy blocks / filters access to all social networking sites. Lady Aisha Academy also encourages parents with children under the ages of 13 to follow the guidance of social media sites such as Facebook and not give their child access. Any such sites found by the school during their duty will be reported to parents and the website in question will be informed of the account and a request made for its removal.

Social media sites have many benefits, however both staff and pupils should be aware of how they present themselves online. Pupils are taught through the IT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. They are educated on the dangers of social networking sites and how to use them in safe and productive ways. Pupils are also advised never to give out personal details of any kind which may identify them or their location. Lady Aisha Academy does not allow the use of social networking sites in school and these sites are blocked using the software Untangle. Staff members are advised to see the Code of Conduct for Staff for guidance on how to conduct themselves on social media platforms.

Mobile phones and personal mobile electronic devices (Smartphones), including wearable technology

Mobile phones and other personal devices are now an important part of everyone's life and have considerable value, particularly in relation to individual safety. Whilst these devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are that:

- they can make pupils and staff more vulnerable to cyberbullying;
- they can be used to access inappropriate internet material;
- they can be a distraction in the classroom;
- they are valuable items that could be stolen, damaged, or lost;
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

Lady Aisha Academy does not allow students to bring smartphones to school. Students may bring a simple handset to school which is handed in to the office upon arrival and retrieved when leaving. Staff members may keep their smartphone on them at all times which must be used responsibly. Further details on expectations regarding mobile phones for pupils can be found in the Pupil Agreement and for staff members, in the Code of Conduct.

Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies to prevent and tackle bullying are set out in the school's Behaviour policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to all members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

Any incidents of cyberbullying will be dealt with in accordance with Lady Aisha Academy's Behaviour Policy and, where appropriate, the school's safeguarding and child protection policies and procedures.

Managing emerging technologies

Technology is progressing rapidly and innovative technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational and pedagogical benefits that they might have. The school keeps up-to-date with modern technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Protecting personal data

The school believes that protecting the privacy of staff, pupils, and parents and regulating their safety through data management, control and evaluation is vital to the whole school and individual progress. The school collects personal data from pupils, parents, and staff and processes it to:

- conduct day to day business processes (e.g. Finance, human resources etc.)
- support teaching and learning,
- monitor and report on pupil and teacher progress,
- strengthen pastoral provision.

Lady Aisha Academy takes responsibility for ensuring that any personal data that is collected and processed is used correctly and only as is necessary. Results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of personal data that the school processes. Please see the school's Data Protection policy for further information. Through effective data management we monitor a range of school provisions and evaluate the well-being and academic

progression of the school body, thus ensuring that we are doing all that is possible to support both staff and pupils.

In line with the Data Protection Act 1998 and the EU GDPR regulations 2018, and following principles of good practice when processing data, the school will:

- ensure that data is fairly and lawfully processed;
- process data only for limited purposes;
- ensure that all data processed is adequate, relevant and not excessive;
- ensure that data processed is accurate;
- not keep data longer than is necessary or legally required;
- process the data in accordance with the data subject's rights;
- ensure that data is secure;
- ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of pupils or staff to pass information onto external authorities; for example, Disclosure & Barring Service (DBS), Independent School's Inspectorate, (ISI), Local Authority, Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection please read the school's Data Protection Policy.

Related Documentation

This policy should be read in conjunction with the following policies and publications.

- Staff Handbook
- Code of Conduct for Staff
- Data Protection Policy
- Anti-Bullying Policy
- Pupil Agreement
- Keeping Children Safe in Education (September 2020)
- Behaviour Policy
- Safeguarding and Child Protection Policy
- Complaints procedure

Reviewed by: N Mistry
Review Date: August 2020

Next Review Date: August 2021