Diocese of Salisbury
Academy Trust
'Beyond expectations for all of God's children'

E-SAFETY POLICY

Policy Date: September 2024

Review Date: September 2027

This policy applies to all schools

Contents

1. Overview

1.1 We are committed to using Information Technology and all it offers to promote learning in the most effective and appropriate way at our Academy - for the benefit of our pupils, staff and community. To this end, we have developed this Acceptable Use Policy, to provide safeguards and ensure that all members of our Academy community understand the benefits, risks and what is expected of them when they use IT in the learning environment.

1.2 Our policy consists of:

- Statements outlining our Academy's approach and attitudes towards using Information & Communications Technologies safely and responsibly.
- Clear guidelines and rules for acceptable use of IT.
- There are also Internet Use Agreements, to be signed by parents, staff and pupils

1.3 The E-Safety Policy will operate in conjunction with other policies including those for IT, behaviour, bullying, curriculum, child protection, data protection and security. Each Academy has an e-safety coordinator, usually the IT Leader. This policy and its implementation will be reviewed regularly to ensure that it remains fit for purpose in relation to the following:

- Keeping Children Safe in Education
- Teaching Online Safety in Schools (DfE, 2019)
- Education for a Connected World framework

1.4 The Trust will review this policy regularly and ensure it is implemented consistently across all Trust schools. The Trust will provide guidance and support to schools in implementing effective online safety measures

2. Why Internet Use is Important

2.1 We believe the internet is an essential element in the 21st century life for education, business and social interaction.

2.2 The Academy recognises its duty to provide children with quality Internet access as part of their learning experience.

2.3 Using the internet and IT in general is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.4 Pupils are increasingly using the internet and a range of IT devices outside of Academy life and therefore need to learn how to evaluate information and to take care of their own safety and security.

3. Using the Internet for Learning in Academies

3.1 We teach all of our pupils how to find appropriate information on the internet and how to ensure as far as possible, that they understand who has made this information available and how accurate and truthful it is.

3.2 All staff will receive regular online safety training as part of their safeguarding and child protection training. This will cover topics such as:

- The 4 Cs of online safety (Content, Contact, Conduct, Commerce)
- Recognising and responding to online risks
- Supporting pupils to use technology safely
- The school's policies and procedures around online safety

Teachers carefully plan all internet-based teaching and lessons to ensure that pupils are focused and using appropriate and relevant materials.

3.3 Children are taught how to use search engines and how to evaluate internet-based information as part of the IT curriculum, and in other curriculum areas where necessary.

3.4 Pupils are taught what internet use is acceptable and what is not and given clear objectives for internet use.

3.5 Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

3.6 Pupils in Key Stage 1 will not be permitted to 'free-surf' the web. In Key Stage 1 and typically in Key Stage 2, pupils' internet access will be through a selection of evaluated sites suitable for the purposes of the task.

3.7 Processes are in place for dealing with any unsuitable material that is found during internet use (see section on managing filtering).

3.8 Where pupils are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit. Pupils who need to search individually will be in the upper primary years. Teachers, wherever possible, will have viewed the content prior to use to check its relevance and suitability.

3.9 The Academy's internet access includes filtering appropriate to primary age pupils which is provided by an approved supplier.

3.10 The Academy may allow the pupils to access the internet at lunchtime as part of a range of activities for young people. There are clear guidelines (see appendix 1) as to what is accessed and it is monitored by the SLT on duty at lunchtime, regulated in access by the teaching staff and supported by specialist IT support staff.

4. Evaluating Internet Content

4.1 The Academy will ensure that staff and pupils are mindful of copyright regulations when copying, downloading and representing materials from the internet. Web-based resources have similar copyright status to printed and recorded materials, such as books, films and music, and this must be taken into consideration when using them.

4.2 Pupils, during Key Stage 2, will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

4.3 Pupils will be taught how to carry out simple checks for bias and misinformation.

4.4 Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

5. Internet Use by Staff

5.1 Our Academy understands that the internet is a valuable resource for Academy staff. It provides a wealth of resources, teaching materials and information that we can use to support and enhance learning. It allows staff to share resources with other academies, and to engage in debate and discussion on educational topics and news.

5.2 It also provides an efficient way to access information from the Department for Education and other government agencies and departments that will help staff to keep abreast of national and local developments.

5.3 There are also increasing opportunities for staff to access INSET and Collaborative Professional Learning activities using the Internet and e-learning resources.

5.4 We are committed to encouraging and supporting our Academy staff to make the best use of IT and all the opportunities it offers to enhance our teaching and support learning.

5.5 Staff use of the internet on Academy computers will be responsible and legal at all times and in keeping with their professional role and responsibility. Misuse of the internet and Academy computer systems will be rigorously investigated.

5.6 Staff must adhere at all times to the Code of Conduct and associated policies within the Employment Manual such as the IT Acceptable Use Policy, AI Use Policy, Social Media Policy and the Communications Policy.

6. E-mail

6.1 Whilst email applications and other messaging systems are not accessed directly by pupils in school, pupils are taught strategies to deal with inappropriate emails and messages and are reminded of the need to write clearly and correctly, not including any unsuitable or abusive material.

6.2 Pupils are taught not to reveal personal details of themselves or others in e-mail communication, nor to arrange to meet anyone without specific permission.

6.3 Staff and governors should use the Academy email service and accounts that are available through Office 365. They are more secure and are easier to access by a third party should the need for scrutiny arise. The secure configuration of this cloud-hosted service aligns with government guidance. Personal web-based email accounts should not be used for professional communications.

6.4 Staff should always ensure that they represent the Academy in a professional and appropriate way when sending email, contributing to online discussions or posting to public websites. Failure to do so could lead to disciplinary action being taken.

6.5 Staff email addresses will be removed by Academy administrative staff, in conjunction with our IT providers, the day following their last day of employment in the Academy. Network access and user accounts will also be suspended at the same time.

6.6 Staff must adhere at all times to the Code of Conduct and associated policies within the Employment Manual such as the IT Acceptable Use Policy, AI-Use Policy, Social Media Policy and the Communications Policy.

6.7 The same principles will apply in respect of other means of communication and social media.

7. Published Content and the Academy Website

7.1 The contact details on the Academy web site will be the Academy address, e-mail and telephone number.

7.2 Individual personal contact information will not be published.

7.3 The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. It will be the responsibility of other staff, personally or by delegation to update the website regularly.

7.4 The Academy maintains a separate website policy and has a clear policy attached to its website.

8. Publishing Pupils' Images and Work

8.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images and video that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images / video on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

8.2 The Academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

8.3 Staff are allowed to take digital / video images to support educational aims, but must follow the Academy policy concerning the sharing, distribution and publication of those images which states that:

- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute or danger;
- Nobody should take, use, share, publish or distribute images of others without their permission;

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images;
- Pupils' full names will not be used anywhere on the website or learning platform, particularly in association with photographs;
- Parents or carers are informed of our policy on publishing and are able to opt their children out.

9. Communication Technologies – Including Chat, Forums, Blogs, Instant Messenger Services, Social Networking Sites

9.1 Most of these modes of electronic communication are restricted in the Academy however they are being used more frequently by pupils and staff outside of the Academy.

9.2 We acknowledge social networking sites, blogs, instant messenger services, chat rooms and forums are beneficial for communication, learning and research. They also present a range of personal safety and privacy issues.

9.3 In Academy time, pupils and staff are not permitted to access social networking sites, public chat rooms, discussion groups and forums etc. for personal use, using Academy resources. Most are blocked by the filtering service used by the Academy.

9.4 Parents and carers will be made aware of their responsibilities regarding their use of social networking

i. Parents are not expected to post pictures of pupils other than their own children on social networking sites
ii. Parents should make complaints through official school channels rather than posting them on social networking sites
iii. Parents should not post malicious or fictitious comments on social networking sites about any member of the school community

9.5 If a pupil or parent is found to have posted libellous or defamatory comments on social networking sites the Headteacher/senior leader is likely to meet with the parents to request that the materials are taken down. The Headteacher/senior leader may explain how this behaviour can have a detrimental impact on the school and potentially their children's education while not allowing the school to actually address the concerns. If the meeting is unsuccessful the headteacher may:

i. Report the parent to the website host with a request to get the material removed
ii. Ban parents from the school site for making abusive or unfounded comments about staff
iii. In serious cases, the school will also consider its legal options (section 1 of the Defamation Act 2013, an individual is guilty of an offence when s/he publishes a statement that causes, or is likely to cause, serious harm to the reputation of the claimant)

9.6 Staff must adhere at all times to the Code of Conduct and associated policies within the Employment Manual such as the IT Acceptable Use Policy, Social Media Policy and the Communications Policy. The AI Use Policy must also be adhered to.

10. Mobile Phones and Other Handheld Devices (including those that are internet enabled)

10.1 Many of our pupils have access to internet-enabled devices such as mobile phones or other hand-held devices which are capable of browsing and uploading to the internet, accessing email and social networking services, as well as taking photos and recording video.

10.2 The Academy recognises the potential advantages these devices can offer for staff and pupils and there are clear and enforceable rules for their use.

10.3 Pupils are taught the legal and moral implications of posting photos and personal information from mobile phones to public websites and how to use these technologies in a safe and responsible manner.

10.4 Children must not bring mobile phones to the Academy. Only in exceptional, prior arranged circumstances will the Academy permit mobile phones belonging to pupils on the Academy premises during Academy sessions. If such a set of circumstances is deemed necessary, the mobile phone will be kept securely by the office or the pupil's class teacher, in accordance with the Academy's arrangements.

10.5 Whilst it is recognised that staff will bring personal mobile devices to work with them, these should not be used around children and in classrooms. They should only be used in offices and areas for staff use and only at suitable times. At no time should they be used to distract staff from teaching and learning, as well as supervising children in an appropriate manner. Staff should never take or make calls when they have children in their care. The Acceptable Use Policy provides further detail in this respect.

10.6 Staff should represent the Academy in a professional and appropriate way when communicating via the internet, contributing to online discussions or posting to public websites using Academy facilities.

10.7 Staff must adhere at all times to the Code of Conduct and associated policies within the Employment Manual such as the IT Acceptable Use Policy, Social Media Policy and the Communications Policy.

11. Electronic Communications with Children by Staff

11.1 Communication between children and Academy staff should take place within clear and explicit professional boundaries.

11.2 When delivering remote learning, staff will follow the school's risk assessment and the Trust's code of conduct. Video conferencing will only take place using approved school platforms. Staff and pupils will be given clear guidelines on appropriate online behaviour and keeping themselves safe during remote learning activities.

11.3 Staff must be careful not to share any personal information with children such as email, web-based communication facilities, home or mobile numbers. They should not request, or respond to, any personal information from the child / young person, other than that which might be appropriate as part of their professional role.

11.4 Staff should ensure that all communications are transparent and open to scrutiny. In addition, all staff must be sure of their social networking and uphold professional confidentiality at all times. Staff should not accept parents or pupils as 'friends' on social contact sites such as Facebook.

11.5 Staff must adhere at all times to the Code of Conduct and associated policies within the Employment Manual such as the IT Acceptable Use Policy, AI-Use Policy, Social Media Policy and the Communications Policy.

12. Downloads

12.1 The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of Academy equipment.

12.2 Pupils are not allowed to download any material from the internet unless directed to do so by an appropriate staff member.

12.3 Staff should take care that files from both other computers outside the Academy and internet are checked for virus contamination before they are used on the Academy system.

12.4 Pupils are not allowed to use CDs, DVDs or memory sticks brought from home or, for example, from magazines unless they have been given permission.

12.5 The Academy subscribes to suitable antivirus software. The software is updated regularly and virus detection is monitored by the Academy's technician.

13. Managing Filtering

13.1 The school uses appropriate filtering and monitoring systems to protect pupils from harmful online content, in line with the Prevent duty and KCSIE requirements. These systems are regularly reviewed for their effectiveness.

13.2 Whilst filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter. Pupils are taught to always report such experiences directly to an adult at the time they occur, and staff receive training to report incidents in accordance with policy, so that action can be taken.

13.3 The action will include:

i. Making a note of the website and any other websites linked to it;
ii. Informing the IT leader and Headteacher;
iii. Logging the incident;
iv. Informing the Internet Service Provider so that the website can be added to the content filter if appropriate;
v. Support is offered to the pupil, including discussion with the pupil about the incident, and how they might avoid similar experiences in future.
vi. Parents will be informed where necessary.
vii. Evaluation of the system and processes will take place to achieve a constructive resolution.

13.4 The Trust will work with the local authority, CEOPS and our Internet Service Provider to ensure systems to protect pupils and staff are effective and appropriate.

13.5 Pupils or staff who deliberately try and access unsuitable materials will be dealt with in accordance with the Academy's discipline policies for pupils and staff.

14. Managing Emerging Technologies, Video-Conferencing and Electronic Resources for Learning

14.1 Emerging technologies and resources (including Artificial Intelligence applications) will be examined for educational benefit and a risk assessment will be carried out before use in the school is permitted in accordance with the Trust's AI Use Policy.

15. Gaming and Other Technologies

15.1 On-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), should not be accessed by pupils unless they have permission from a member of staff to do so.

15.2 Academies will be required to educate children, and inform parents, as to how and why games may or may not be age appropriate.

15.2 Staff must adhere at all times to the Code of Conduct and associated policies within the Employment Manual such as the IT Acceptable Use Policy, Social Media Policy and the Communications Policy. Staff are not expected to use on-line gaming or gambling systems.

16. Online Bullying and Harassment (Cyberbullying)

16.1 Online bullying and harassment via Instant messaging, chat rooms, social networking sites etc. are potential problems that can have an effect on the well being of pupils and staff alike.

16.2 Cyberbullying will be treated as seriously as any other form of bullying. The school will follow the anti-bullying procedures outlined in the behaviour policy when responding to cyberbullying incidents. Staff will be vigilant in monitoring for signs of cyberbullying and will report concerns following the child protection procedures.

16.3 Our Academy has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. These include:

- No access in the Academy to public chat-rooms, instant messaging services and social networking sites;
- Pupils are taught how to use the internet safely and responsibly which includes how to identify and respond to 'cyberbullying';
- Children are taught how and where to report incidents that make them feel unhappy or worried;
- As with any form of bullying, we encourage pupils to discuss with staff any concerns or worries they have about online bullying and harassment.

17. Authorising Internet Access

17.1 All staff must read 'Acceptable IT Use Agreement' before using any Academy IT resource.

17.2 Use by visitors will be subject to monitoring. Guest logins must be used for visitors rather than being given access details belonging to someone else.

17.3 At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. Parents are asked to sign and return a consent form when their child starts at the Academy.

18. Assessing Risks

18.1 The 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 an Academy computer.

18.2 The Academy can't accept liability for the material accessed, or any consequences of Internet access.

18.3 The Academy will audit IT provision to establish if the E-safety policy is adequate and that its implementation is effective.

18.4 Any pupil found to be at risk of harm will be supported in accordance with statutory guidance.

19. Handling E-Safety Complaints

19.1 Any complaint about staff misuse must be referred to the Headteacher.

19.2 Complaints of a child protection nature must be dealt with in accordance with the Academy child protection procedures.

19.3 Pupils and parents will be informed of the complaints procedure.

20. Introducing the E-Safety Policy to Pupils

20.1 E-safety rules will be shared widely rooms and discussed with pupils regularly.

20.2 Pupils will be informed that network and Internet use can be monitored.

21. Staff and the E-Safety policy

21.1 All staff will be given access to the Academy E-Safety Policy and its importance will be explained. A programme of E-safety training will be available to staff who can also discuss matters with the E-Safety Coordinator on an ad-hoc basis.

21.2 Staff should be aware that internet traffic can be monitored and traced to the individual user.

21.3 Discretion and professional conduct is essential.

21.4 All new staff should receive E-safety training as part of their induction programme, ensuring that they fully understand the Academy Acceptable Use Policy.

21.5 The E-Safety Coordinator will receive regular updates through attendance at training sessions and/or by reviewing guidance documents released by appropriate authorities and providers.

21.6 The Academy will ensure compliance with the "Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance".

This includes implementing robust filtering and monitoring systems to safeguard pupils and staff from inappropriate content and online threats.

22. Enlisting Parental Support

22.1 Some parents and carers might have a limited understanding of E-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of children's on-line experiences.

22.2 Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

22.3 The Academy provides information and awareness to parents and carers through:

- Information in Academy newsletters;
- Links to resources from the Academy website;
- Parent workshops.

23. Academy Standards and Ethos Committee (ASEC) Members (Governors)

23.1 ASEC members should take part in e-safety training / awareness sessions, with particular importance for those who are involved in monitoring IT / E-safety/ health and safety / child protection.

23.2 This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governor Association or other relevant organisation;
- Participation in Academy training / information sessions for staff or parents.

23.3 ASEC members should use the Academy email address provided to them in order to carry out communications in respect of the Academy.