Date of last review	November 2023	Review period	Annually
Date of next review	November 2024	Owner	CEO

Online Safety Policy

Enabling a world of freedom, opportunity and fulfilment

History of Policy Changes

Date	Page	Change	Origin of Change

Contents

Introduction

Salisbury Sixth Form College (the 'Academy') recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all pupils, staff, Governors and Trustees will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility.

All staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping pupils and young people navigate the online world safely and confidently.

Responsibilities

The **Academy Leader** is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the Academy. All breaches of this policy must be reported to the Academy Leader.

The **Online Safety Lead** is assigned to the Designated Safeguarding Lead post in the college.

The Designated Safeguarding Lead takes lead responsibility for online safety in the Academy, in particular:

- Supporting staff to understand this policy and that it is being implemented consistently throughout the Academy
- Working with staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the Academy's Child Protection and Safeguarding Policy
- Ensuring that any online safety incidents are logged in the safeguarding system and dealt with appropriately in line with the safeguarding policy
- Ensuring that any incidents of cyberbullying are logged on the safeguarding system and dealt with appropriately and in line with the Academy behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in Academy to the Academy Leader and the Academy Governance Committee (AGC).

The Trust's dedicated ICT supplier is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at the Academy, including terrorist and extremist material
- Ensuring that the Academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the Academy's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Provide monthly user reports on all activities the academy's designated safeguarding lead and academy leader
- This list is not intended to be exhaustive.

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the Academy's ICT systems and the internet and ensuring that pupils follow the Academy's terms on acceptable use (See Appendices)
- Working with the DSL to ensure that any online safety incidents are logged on the safeguarding system and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the Academy's behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- This list is not intended to be exhaustive.

The Academy works closely with **parents/carers** to help ensure that pupils can use internet, mobile and digital technologies safely and responsibly both at home and in the college. The Academy will inform parents/carers about what their children are being asked to do online, including the sites they will be asked to access and who from the Academy (if anyone) their child will be interacting with online.

The support of parents/carers is essential to implement the online safety policy effectively and help keep pupils safe. It is important that parents/carers understand the crucial role they play in this process. The Academy seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The Academy provides regular updated online safety information through the Academy website, newsletters and by other means.

Parents/carers are asked on an annual basis to read, discuss and co-sign with each child the Acceptable Use Agreement.

Parents are asked to notify a member of staff or the Academy Leader of any concerns or queries regarding online safety

- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
  What are the issues? - UK Safer Internet Centre
  Help & advice | Childnet
  Parents and Carers resource sheet | Childnet

Organisations that are renting space from the Academy and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the Academy network, cloud-based services and/or equipment then they must adhere to the Academy's online safety procedures and acceptable use agreements. If the organisation is operating in Academy time or when students are on site in the care of the Academy, then the safeguarding of students is paramount and the organisation must adhere to the Academy's online safety procedures and acceptable use agreements.

Scope of Policy

The policy applies to:

- students
- parents/carers
- teaching and support staff
- Academy Governors
- Trustees
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the Academy's facilities.

The Academy also works with partners and other providers to ensure that students who receive part of their education off site or who are on a college trip or residential are safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole Academy community. It is linked to the following Academy policies and documents:

- Safeguarding and Child Protection Policy, Keeping Children Safe in Education, GDPR, Behaviour Policy and Procedures, Anti-bullying Policy, PSHE/RSE policies.

Curriculum

Online safety is fully embedded within our curriculum. The Academy provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The Character Curriculum is central in supporting the delivery of online safety education. The character curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for students to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Students are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies.

The Academy Character Curriculum includes areas such as:

- recognising fake news and extremism Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.
- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- How the law can help protect against online risks and abuse

The Academy recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the Academy Leader.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Academy Behaviour Policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The Academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/ tutors will discuss cyber-bullying with their class/tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, Governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. The Academy also distributes information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support pupils who may be affected.

In relation to a specific incident of cyber-bullying, the Academy will follow the processes set out in the Academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the Academy will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so. The Academy seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The Academy expects everyone to use internet, mobile and digital technologies responsibly and strictly in accordance with the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of the Academy for students, parents/carers, staff and Governors and all other visitors to the Academy.

Examining electronic devices

The Academy Leader, and any member of staff authorised to do so by the Academy Leader, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the Academy rules as a banned item for which a search can be carried out, and/or is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the Academy Leader / DSL / appropriate staff member
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or undermine the safe environment of the Academy or disrupt teaching, and/or commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Academy Leader / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may ask the owner to delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or the pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next.

The DSL will make the decision in line with the DfE's latest guidance on Searching, screening and confiscation in schools - GOV.UK (www.gov.uk) and the UK Council for Internet Safety (UKCIS) guidance on Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk) and the Academy's behaviour policy.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the Academy's complaints procedure.

Acceptable use of internet in the Academy

All pupils, parents, staff, volunteers and Governors are expected to sign an agreement regarding the acceptable use of the Academy's ICT systems and the internet (Appendices A to E)

Visitors will be expected to read and agree to the Academy's terms on acceptable use if relevant.

Use of the Academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, Governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements.

Use of email

Staff, Governors and Trustees should use an Academy email account for all official Academy communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact students, parents or conduct any Academy business using a personal email address.

Pupils should use Academy approved accounts on the Academy system for educational purposes. Where required parent/carer permission will be obtained for the pupil account to exist. Emails created or received as part of any Academy role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, Governors, Trustees and pupils should not open emails or attachments from suspect sources and should report their receipt to Support@oakforduk.com.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

Staff must preview sites, software and apps before their use in the Academy or before recommending them to students.

Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required.

If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.

Staff must only use pre-approved systems if creating blogs, wikis or other online content.

When working with students, searching for images should be done through Google Safe Search Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the Academy or Trust or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect
- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the Academy
- Use the Academy's hardware and Wi-Fi facilities for running a private business

- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the Academy

Use of personal mobile devices (including phones)

The Academy allows staff, including temporary and peripatetic staff, students and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the Academy allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on Academy premises or on off-site Academy events and activities of anyone other than their own child, unless there is a pre-specified permission from the Academy Leader. When a parent/carer is on Academy premises but not in a designated area, their phone/s must be switched off and out of sight.

In secondary academies, pupils are allowed to bring in personal mobile devices/phones but must not use them for personal purposes within lesson time. Phones will be locked in Yonder cases and unlocked at the end of the academic day. In Primary academies, mobile phones must be turned off, and handed in to the office at the beginning of the Academy day and collected at the end of the Academy day. Users bringing personal devices into the Academy must ensure there is no inappropriate or illegal content on the device.

Under no circumstances should students use their personal mobile devices/phones to take images of any other pupil (unless they and their parents have given agreement in advance), any member of staff

The Academy is not responsible for the loss, damage or theft of any personal mobile device that is brought onto Academy premises.

Reporting incidents, abuse and inappropriate material

There may be occasions in the Academy when either a student or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the student or adult must report the incident immediately to the first available member of staff, the DSL or the Academy Leader. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The Academy takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

Staff, Governor and Trustee Training

Staff, Governors and Trustees are trained to fulfil their roles in online safety. The Academy audits the training needs of all Academy staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the Academy's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with pupils and based on the Academy premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B).

Guidance is provided for occasional visitors, volunteers and parent/carer helpers.

Appendix A – Online Safety Acceptable Use Agreement - Staff, Governors, Trustees and Student Teachers (on placement or on staff)

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the Academy. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities. All staff, student teachers and Governors are expected to adhere to this agreement and to the online safety policy.

Any concerns or clarification should be discussed with the Academy DSL or Academy Leader. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

When using the Academy's ICT systems and accessing the internet in the Academy, or outside the Academy on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) or access social media or chat rooms
- Use them in any way which could harm the Academy's reputation
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the Academy's network
- Share my password with others or log in to the Academy's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the Academy, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the Academy

I will only use the Academy's ICT systems and access the internet in the Academy, or outside the Academy on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the Academy will monitor the websites I visit and my use of the Academy's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the Academy, and keep all data securely stored in accordance with this policy and the Academy's data protection policy.

I will let the Designated Safeguarding Lead (DSL) and Academy Leader know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the Academy's ICT systems and internet responsibly and ensure that students in my care do the same**.**

Signed: **Date**

Appendix B - Primary Pupil Online Safety Agreement

When I use the Academy's ICT systems (like computers) and get onto the internet in Academy I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    a. I click on a website by mistake or I receive messages from people I don't know
    b. I find anything that may upset or harm me or my friends
- Use Academy computers for Academy work only
- Be kind to others and not upset or be rude to them
- Look after the Academy ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the Academy network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the Academy will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed:

Date:

Parent/Carer agreement: I agree that my child can use the Academy's ICT systems and internet when appropriately supervised by a member of Academy staff. I agree to the conditions set out above for pupils using the Academy's ICT systems and internet and will make sure my child understands these.

Signed:

Date:

Appendix C - Online Safety Acceptable Use Agreement Secondary Pupils

When I use the Academy's ICT systems and internet in the Academy:

- I will only use Academy IT equipment for Academy purposes and will not access personal accounts.
- I will not download or install software on Academy IT equipment.
- I will only log on to the Academy network, other Academy systems and resources using my own Academy user name and password.
- I will not reveal my passwords to anyone other than a parent/carer.
- I will make sure that all my electronic communications are responsible and sensible.
- I understand that everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers, parents/carers and the police if necessary. I know it is essential that I build a good online reputation.
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of staff if I am in the Academy, or parent/carer if I am not in the Academy.
- I will not give out my own or others' personal information, including: name, phone number, home address, interests, Academy name or clubs or any personal image. I will report immediately any request for personal information, to a member of staff if I am in the Academy or parent/carer if I am not in the Academy.
- I should never post photographs, videos or livestream without the permission of all parties involved.
- I will not upload any images, videos, sounds or words that could upset, now or in the future, any member of the Academy community, as this is cyberbullying.
- I will be respectful to everyone online; I will treat everyone the way that I want to be treated. I will ensure that all my online activity, both in and outside the Academy, will not cause distress to anyone in the Academy community or bring the Academy into disrepute.
- I will not respond to hurtful behaviour online but will report it. I have the right to block and will say no to any inappropriate or upsetting request.
- I will respect the privacy and ownership of others' work on-line and will adhere to copyright at all times.
- I will not attempt to bypass the internet filtering system in the Academy.
- I will not assume that new technologies can be brought into the Academy and will check with staff before bringing in any device.
- I will not lie about my age in order to sign up for age inappropriate games, apps or social networks.
- I understand that not everything I see or hear online is true, accurate or genuine. I also know that some people on the internet are not who they say they are and may have ulterior motives for assuming another identity that will put me at risk. I will gain permission from parents/carers before arranging to meet someone I only know on the internet.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules, teachers will investigate, I may be disciplined and my parents/carers may be contacted. If I break the law the police may be informed.

Signed:

Date:

Parent/Carer agreement: I agree that my child can use the Academy's ICT systems and internet when appropriately supervised by a member of Academy staff. I agree to the conditions set out above for pupils using the Academy's ICT systems and internet and will make sure my child understands these.

Signed:

Date:

Appendix D – Information and Requirements for Visitors, Volunteers and Parent/Carer Helpers

Academy Name: Salisbury Sixth Form College

Online safety lead: Craig Chambers

Designated Safeguarding Lead (DSL): Craig Chambers

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the Academy and other aspects of safeguarding in connection with online safety.

Please raise any safeguarding concerns arising from your visit immediately with the Academy Leader and/or DSL

• I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.

• I will not take images, sound recording or videos of Academy events or activities, on or off site, on any device. Any possible exception must be pre-arranged.

• I will not give out my personal details such as mobile phone number, email address, and social media account details to students. Where appropriate I may share my professional contact details with parents/carers provided the DSP or Academy Leader is informed before I leave the Academy.

• I understand my visit to the Academy may give me access to privileged information about pupils, staff, Academy systems and plans. Such information should never be shared on line, including on social media sites.

• I understand I should not use Academy equipment to access the internet without prior approval from my contact in the Academy or the Academy Leader.

• If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet whilst in the Academy. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the Academy.