St Aldhelm's Academy
The best in everyone™
Part of United Learning

Online Safety Policy

St Aldhelm's Academy
The best in everyone™

Contents

1. Policy Section 1 3

1.1. Policy detail 1 ..... **Error! Bookmark not defined.**

1.2. Policy detail 2 ..... **Error! Bookmark not defined.**

1.3. Policy detail 3 ..... **Error! Bookmark not defined.**

1.4. Policy detail 4 ..... **Error! Bookmark not defined.**

1.5. Policy detail 5 ..... **Error! Bookmark not defined.**

2. Policy Section 2 ..... **Error! Bookmark not defined.**

2.1. Policy detail 6 ..... **Error! Bookmark not defined.**

2.2. Policy detail 7 ..... **Error! Bookmark not defined.**

2.3. Policy detail 8 ..... **Error! Bookmark not defined.**

2.4. Policy detail 9 ..... **Error! Bookmark not defined.**

2.5. Policy detail 10 ..... **Error! Bookmark not defined.**

3. Policy Section 3 ..... **Error! Bookmark not defined.**

3.1. Policy detail 11 ..... **Error! Bookmark not defined.**

3.2. Policy detail 12 ..... **Error! Bookmark not defined.**

3.3. Policy detail 13 ..... **Error! Bookmark not defined.**

3.4. Policy detail 14 ..... **Error! Bookmark not defined.**

3.5. Policy detail 15 ..... **Error! Bookmark not defined.**

4. Policy Section 4 ..... **Error! Bookmark not defined.**

4.1. Policy detail 16 ..... **Error! Bookmark not defined.**

4.2. Policy detail 17 ..... **Error! Bookmark not defined.**

4.3. Policy detail 18 ..... **Error! Bookmark not defined.**

4.4. Policy detail 19 ..... **Error! Bookmark not defined.**

4.5. Policy detail 20 ..... **Error! Bookmark not defined.**

1. Policy Aims

The purpose of this online safety policy is to:

- Safeguard and protect all members of St Aldhelm's Academy community online.
- To raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

St Aldhelm's Academy identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
- Commerce: Financial risks like Phishing scams, gambling, or misleading advertisements.

St Aldhelm's Academy believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and all staff are protected from potential harm online.

St Aldhelm's Academy identifies that the internet and associated devices, such as computers, tablets, mobile phones, smart watches and games consoles, are an important part of everyday life.

St Aldhelm's Academy believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of St Aldhelm's Academy (collectively referred to as "staff" in this policy) as well as learners, parents and carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with academy issued devices for use off-site, such as a work laptops, tablets, smart watches or mobile phones.

This online safety policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education , 'Working Together to Safeguard Children' 2024, As well as DFE guidance 'Sexual violence and sexual harassment between children in schools and colleges', 'Sharing nudes-semi nudes: advice for educational settings working with children and young people'

2. Monitoring and Review

Technology in this area evolves and changes rapidly. St Aldhelm's Academy will review this policy as required.

The policy will be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure

We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure they have oversight of online safety, the Principal/DSL will be informed of online safety concerns, as appropriate.

3. Roles and Responsibilities

The Vice Principal for Behaviour and Safeguarding has lead responsibility for online safety. St Aldhelm's Academy recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

3.1. The Leadership Team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct policy which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

3.2. The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the academy's safeguarding responsibilities and that a coordinated approach is implemented.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Report online safety concerns, as appropriate, to the Vice Principal or Principal.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually).
- Meet regularly with the governor with a lead responsibility for safeguarding.

3.3. It is the responsibility of all members of staff to:

- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the academies safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

3.4. It is the responsibility of staff managing the technical environment to:

- Implement appropriate security measures as directed by the leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

3.5. It is the responsibility of all learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Read and adhere to the acceptable use policies. Respect the feelings and rights of others both on and offline. Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues. The following are not permitted:
    - Sending or displaying offensive messages or pictures
    - Using obscene language
    - Harassing, insulting or defaming the character of others ("cyber-bullying")
    - Damaging computers, computer systems or computer networks
    - Violating copyright laws
    - Using another pupil's logon account
    - Trespassing in another pupil's folders, work or files
    - Attempting to hack into the system
    - Attempting to install, or play games other than those sanctioned by staff members
    - Recording digital images of any member of the academy community without permission Sanctions

Violations of the above rules will be dealt with via the Academy behaviour policy.

3.6. The academy has installed computers with Internet access to help our learning. These rules will help to keep you safe and help us be fair to others.

- I will only access the system with my own login and password, which I will keep secret
- I will not access another person's user area, or interfere with other people's work or computer files
- I will not behave in a way that can cause damage to ICT equipment or to software installations.
- I will not bring in software from home or make a copy of academy software without permission from a member of staff
- I will ensure I have permission from a member of staff before using the Internet or taking digital images of others in the academy; digital images are to be used only in academy projects with the permission of the subject and must not be circulated or published in any way.
- I will only use academy E-mail for projects my teacher has approved
- The messages I send will be polite and responsible
- I will not use ICT systems to threaten, insult or defame the character of others
- I will not give my home address or telephone number to outside people, or arrange to meet someone, unless my parents/carers and/or teacher has given permission (e.g. Curriculum Vitae)
- I will report any unpleasant material or messages sent to me.
- I understand that the academy may check my computer files and may monitor the Internet sites I visit

3.7. It is the responsibility of parents and carers to:

Read the acceptable use policies and encourage their children to adhere to them.
Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.

- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement and acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the academy, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

4. Education and Engagement Approaches

4.1. Education and engagement with learners.

The academy will embed online safety across the curriculum to raise awareness and promote safe and responsible internet use amongst all learners by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in, SMSC, Personal, Social, Health and Economic (PSHE), assemblies and tutor time as well an across curriculum education approach.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating all learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching all learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

The academy will support all learners to read and understand the acceptable use policies in a way which suits their age and ability by:

- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Implementing appropriate peer education approaches.
- Providing online safety education and training as part of the transition programme across the key stages.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

4.2. Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
  • Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will be delivered as part of existing safeguarding and child protection training/updates.
  Updates/training will also be shared through staff briefing as required Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
  • Make staff aware that our IT systems are monitored; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
  • Make staff aware that their online conduct outside of the academy, including personal use of social media, could have an impact on their professional role and reputation.

4.3. Awareness and engagement with parents and carers

St Aldhelm's Academy recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats.
- Drawing their attention to the online safety policy and expectations in newsletters, letters and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
- Requiring them to read our acceptable use policies and discuss the implications with their children.

5. Reducing Online Risks – the four C's

There are four categories of risk with online safety:

- Content
- Contact
- Conduct
- Commerce

In order to reduce the risks associated with being online we will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Content - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Contact - educate children on the risks associated with being in contact with other online users to prevent the likelihood of students being at risk of grooming, exploitation, talking to 'fake people' and impersonators.
- Conduct – educate people on the law and the implications for sending and receiving inappropriate and explicit online images and online and how to report receiving these messages and pictures.
- Commerce – educating young people on the risks of phishing, advertising, online gambling and financial scams.

6. Use of Generative Artificial Intelligence (AI)

St Aldhelm's Academy recognises that generative artificial intelligence (AI) tools (such as text, image or code generators) are increasingly accessible to children and young people.

The academy will educate learners on the safe, ethical and responsible use of AI, including:

- Understanding the limitations of AI-generated content and the risk of misinformation
- Avoiding plagiarism and misuse in academic work
- Safeguarding risks, including impersonation, manipulation and inappropriate content generation
- Data protection and the risks of sharing personal information with AI platforms

Staff will receive guidance on the appropriate professional use of generative AI, ensuring that its use:

- Supports learning rather than replaces critical thinking
- Does not compromise safeguarding, assessment integrity or data protection
- Aligns with academy policies, including safeguarding, acceptable use and behaviour

Any misuse of generative AI that raises safeguarding concerns will be managed in line with this Online Safety Policy and the academy's safeguarding procedures.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through education and training approaches.

7. Password Policy

All members of staff will have their own unique username and passwords to access our systems; members of staff are responsible for keeping their password private.

All learners are provided with their own unique username and passwords to access our systems; learners are responsible for keeping their password private.

We require all users to:

- Always keep their password private; users must not share it with others.
- Not to login as another user at any time.

8. Social Media

8.1. The expectations' regarding safe and responsible use of social media applies to all members of St Aldhelm's Academy community.

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the academy.
- All members of staff are to safeguard themselves and their privacy when using social media sites.
- All members of staff should carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role. Communicating with learners and parents and carers
- All members of staff should not communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions that may compromise this should be discussed with the DSL (or deputy).
- Any communication from learners and parents received on personal social media accounts must be reported to the DSL (or deputy) immediately.

8.2. Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to all learners as part of an across curriculum education approach.
- Any concerns regarding learner's use of social media will be dealt with in accordance with existing policies, including anti-bullying peer on peer and behaviour policies.
- Concerns will be shared with parents/carers as appropriate
- Learners will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.

- To use safe passwords. o To use social media sites which are appropriate for their age and abilities. o How to block and report unwanted communications.
- How to report concerns both within the setting and externally?

9. Use of Personal Devices and Mobile Phones/Smart Watches

St Aldhelm's Academy mobile free zone. Students are not to have their mobile phones out at any times. Their mobile phones should remain in their school bags or left at home. If they are seen they will be confiscated and collected at the end of the school day by either the student or the parent depending on what is agreed within the behaviour policy.

9.1. Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches and mobile phones) will take place in accordance with the law and other appropriate policies, such as Code of Conduct, anti-bullying, behaviour and child protection
- Electronic devices of any kind that are brought onto the academy site are the responsibility of the user.
- The sending of abusive or inappropriate messages or content via mobile phones, smart watches or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.

9.2. **Learners Use of Personal Devices and Mobile Phones/Smart Watches**

- All learners will be educated regarding the safe and appropriate use of personal devices, smart watches and mobile phones and will be made aware of boundaries and consequences.
- Mobile phones, smart watches and personal devices must not be taken into examinations.
  - Learners found in possession of a mobile phone, smart watch or personal device during an exam may be withdrawn from that examination.
  - Staff may confiscate a learner's mobile phone, smart watch or device if they believe it is seen in the academy or it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
  - Searches of mobile phone, smart watches or personal devices will only be carried out in accordance with our policy. Content may be deleted or requested to be deleted if it contravenes our policies

9.3. Visitors' Use of Personal Devices and Mobile Phones/Smart Watches

- Visitors (including volunteers and contractors) who are on the academy site for a regular or extended period will use their mobile phones, smart watches and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or Principal of any breaches our policy.

10. Concerns about Learners Welfare

The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.

The DSL (or deputy) will record these issues in line with our Child Protection policy

The DSL (or deputy) will ensure that online safety concerns are reported to relevant agencies

We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

11. Staff Misuse

Any complaint about staff misuse will be referred to the Principal, in accordance with the allegations policy.

Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

Appropriate action will be taken in accordance with our Code of Conduct policy.

12. Procedures for Responding to Specific Online Incidents or Concerns

12.1. Online Sexual Violence and Sexual Harassment between Children

St Aldhelm's Academy recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies as well as KCSIE guidance in Part 5.
    - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as BCP MASH and/or the Police

12.2. Youth Produced Sexual Imagery

St Aldhelm's Academy recognises youth produced sexual imagery as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

We will implement preventative approaches for youth produced sexual imagery via a range of age and ability appropriate education for all learners, staff and parents/carers.

We will follow the advice as set out in the DFE Sharing nudes-semi nudes: advice for educational settings working with children and young people' Sharing nudes and semi-nudes: how to respond to an incident as well as the DFE Sexual violence and sexual harassment between children in schools and colleges'

We will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.

- If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with our child protection policies o Ensure the DSL (or deputy) responds in line with DFE guidance: o Store the device securely.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to BCP MASH and/or the Police, as deemed appropriate in line with the DFE Guidance
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour for learning policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the DFE guidance.
- Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

12.3. Online Child Sexual Abuse and Exploitation (including County Lines)

St Aldhelm's Academy recognises online child sexual abuse and exploitation (including County lines) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).

- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for all learners, staff and parents/carers.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our child protection policies. o If appropriate, store any devices involved securely.
    - Make a referral to the BCP MASH (if required/appropriate) and immediately inform police.
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.

12.4. Online Radicalisation and Extremism

We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.

We will implement preventative approaches for online radicalisation and extremism via a range of age and ability appropriate education for all learners, staff and parents/carers.

If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.

Links with other policies and practices

This policy links with several other academy policies including:

- Anti-Bullying policy
- Behaviour for Learning Policy
- Peer on Peer Abuse Policy
- Child Protection and Safeguarding Policy
- Code of Conduct Preventing the Abuse of Trust Policy

13. Useful Links National Links and Resources

13.1. For Education Settings:

- Department for Education (DFE) http://www.gov.uk/
- Police- 101 or if immediate danger 999
- CEOP: http://www.thinkuknow.co.uk/ http://www.ceop.police.uk/
- Childnet: http://www.childnet.com/
- Internet Matters: http://www.internetmatters.org/
- Internet Watch Foundation (IWF): http://www.iwf.org.uk/
- NSPCC: http://www.nspcc.org.uk/onlinesafety
- ChildLine: http://www.childline.org.uk/
- Net Aware: http://www.net-aware.org.uk/
- UK Safer Internet Centre: http://www.saferinternet.org.uk/
- Professional Online Safety Helpline: http://www.saferinternet.org.uk/about/helpline

13.2. Local Links and Resources for Parents/Carers:

- Local Authority Designated Safeguarding Officer (LADO)
  The main contact details for the LADO service are 01202 817600 or lado@bcpcouncil.gov.uk
- Education Safeguarding Advisor & LADO Julie Murphy: 01202 128744 or juliemurphy@bcpcouncil.gov.uk
- First Response Hub: 01202 123334 or childrensfirstresponse@bcpcouncil.gov.uk
- BCP Family Information Directory - Family Information Directory