Online Safety Policy

Applicable to:	✓	Astley Community High School
	✓	Seaton Sluice Middle School
	✓	Whytrig Middle School
Approval body:	Pupil Support Committee	

Status:

Statutory policy or document	No
Review frequency	Governing Body to determine
Approval by	Governing Body to determine

Publication:

Statutory requirement to publish on school website	No
Agreed to publish on school website	Yes

Review:

Frequency	**Next Review Due**
Annually	Autumn 2024

Version Control:

Author	Creation Date	Version	Status
Information and Curriculum Support Manager (NB)	2 December 2016	0.1	Draft policy for SVF for consultation with SLT
Changed by	**Revision Date**		
Business Manager (SH)	14 December 2016	0.2	Amendments to format etc.
Information and Curriculum Support Manager (NB)	18 January 2017	1.0	Final version for publication
IT & Technical Support Manager (AD)	3 December 2018	1.1	Updated to reflect current systems, including named safeguarding contacts and references to GDPR
Business Manager (BW)	3 January 2019	1.2	Formatting changes
Business Manager (BW)	1 February 2019	2.0	Final approved version for publication
Business Manager (BW)	22 July 2019	2.1	SSMS DSL and all email addresses updated
Business Manager (BW)	28 January 2020	2.2	Annual review; no changes required
Business Manager (BW)	3 February 2020	3.0	Final approved version for publication
Business Director (BW)	28 July 2022	3.1	Fully reviewed and rewritten in line with the Key for School Leaders model policy (June 2022)
Business Manager - ICT and Infrastructure (AD)	29 July 2022	3.2	Minor revisions and clarifications
Business Director (BW)	31 August 2022	4.0	Final approved version for publication
Business Director (BW)	31 August 2022	4.1	Revised 6.9-6.17 in line with updated guidance from the DfE on searching, screening, and confiscation
Business Director (BW)	2 October 2023	4.2	Annual review; updates in line with the Key for Leaders model policy (August 2023) including the potential misuse of generative AI
Business Director (BW)	25 October 2023	4.3	Minor change to roles and responsibilities regarding the logging of incidents
Business Director (BW)	13 November 2023	5.0	Final approved version for publication

1 Aims

1.1 Our federation aims to:

- have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

1.2 Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

1.3 The Seaton Valley Federation believes that online safety (e-safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

1.4 The federation acknowledges that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online. The federation recognises that it has a clear duty to ensure that all children and staff are protected from potential harm online.

1.5 The federation also has a duty to provide the community with quality internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

2 Legislation and guidance

2.1 This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and Cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

2.2 It also refers to the DfE's guidance on Protecting children from radicalisation.

2.3 It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

2.4 The policy also takes into account the National Curriculum computing programmes of study.

3 Roles and responsibilities

Governing Body

3.1 The governing body has overall responsibility for monitoring this policy and holding the Executive Headteacher to account for its implementation.

3.2 The governing body will:

- make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring
- make sure all staff receive regular online safety updates, as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children
- coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Leads (DSLs)
- ensure children are taught how to keep themselves and others safe, including keeping safe online.
- ensure the school has appropriate filtering and monitoring systems in place on federation devices and networks, and regularly review their effectiveness
- review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the federation in meeting those standards, which include:
    - identifying and assigning roles and responsibilities to manage filtering and monitoring systems
    - reviewing filtering and monitoring provisions at least annually
    - blocking harmful and inappropriate content without unreasonably impacting teaching and learning
    - having effective monitoring strategies in place that meet their safeguarding needs

3.3 The governor who oversees online safety is Susan Dungworth.

3.4 All governors will:

- ensure that they have read and understand this policy
- agree and adhere to the terms of the federation's ICT and Internet Acceptable Use Policy
- ensure that online safety is a running and interrelated theme while devising and implementing their whole federation approach to safeguarding and related policies and/or procedures
- ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with

SEND, because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

Executive Headteacher

3.5 The Executive Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the federation.

Designated Safeguarding Leads

3.6 Details of the federation's DSLs and deputies are set out in our Child Protection Policy as well as relevant job descriptions.

3.7 The DSL takes lead responsibility for online safety in school, in particular:

- supporting the Executive Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the federation
- working with the Executive Headteacher and governing body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- taking the lead on understanding the filtering and monitoring systems and processes in place on federation devices and networks
- working with the Business Manager - ICT and Infrastructure to make sure the appropriate systems and processes are in place
- working with the Executive Headteacher, Business Manager - ICT and Infrastructure and other staff, as necessary, to address any online safety issues or incidents
- managing all online safety issues and incidents in line with the federation's Child Protection Policy
- liaising with other agencies and/or external services if necessary
- providing regular reports on online safety in school to the Executive Headteacher and/or governing body
- undertaking annual risk assessments that consider and reflect the risks children face
- providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

3.8 This list is not intended to be exhaustive.

Business Manager - ICT and Infrastructure

3.9 The Business Manager - ICT and Infrastructure 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 school, including terrorist and extremist material
- ensuring that the federation'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 federation's ICT systems on a regular basis

- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files and information
- updating and delivering staff training on online safety

3.10 This list is not intended to be exhaustive.

All Staff and Volunteers

3.11 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 of the federation's ICT and Internet Acceptable Use Policy
- ensuring that pupils follow the terms of the federation's ICT and Internet Acceptable Use Policy
- ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with each school'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'

3.12 This list is not intended to be exhaustive.

Parents/Carers

3.13 Parents/carers are expected to:

- notify a member of staff, the Head of School or the Executive Headteacher of any concerns or queries regarding this policy
- ensure their child has read, understood and agreed to the terms of the federation's ICT and Internet Acceptable Use Policy

3.14 Further guidance on keeping children safe online can be found at Appendix A.

Visitors and Members of the Community

3.15 Visitors and members of the community who use the federation's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms of the federation's ICT and Internet Acceptable Use Policy.

4 Educating pupils about online safety

4.1 Pupils will be taught about online safety as part of the curriculum.

4.2 Pupils in Key Stage 2 will be taught to:

- use technology safely, respectfully and responsibly
- recognise acceptable and unacceptable behaviour
- identify a range of ways to report concerns about content and contact

4.3 In Key Stage 3, pupils will be taught to:

- understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- recognise inappropriate content, contact and conduct, and know how to report concerns

4.4 Pupils in Key Stage 4 will be taught:

- to understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- how to report a range of concerns

4.5 By the end of secondary school, pupils will know:

- their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- what to do and where to get support to report material or manage issues online
- the impact of viewing harmful content
- that specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- that sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- how information and data is generated, collected, shared and used online
- how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- how people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

4.6 The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5 Educating parents/carers about online safety

5.1 The federation will raise parents/carers' awareness of internet safety in communications home, and in information published on our website, including this policy.

5.2 Online safety will also be covered during parents' evenings.

5.3 The federation will let parents/carers know:

- what systems the federation uses to filter and monitor online use

- what their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

5.4 If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School and/or the DSL.

5.5 Concerns or queries about this policy can be raised with any member of staff or the Head of School.

6 Cyberbullying

Definition

6.1 Cyberbullying 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. Please also see each school's Behaviour Policy.

Preventing and Addressing Cyberbullying

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

6.3 Each school will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyberbullying with their classes or tutor groups.

6.4 Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes Spiritual, Moral, Social and Cultural development (SMSC) and personal, social, health and economic (PSHE) education, and other subjects where appropriate.

6.5 All staff, governors and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support pupils, as part of their safeguarding training.

6.6 The federation also sends information on cyberbullying to parents/carers so that they are aware of the signs, how to report it, and how they can support children who may be affected.

6.7 In relation to a specific incident of cyberbullying, the school will follow the processes set out in its Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

6.8 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.

Examining Electronic Devices

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

- poses a risk to staff or pupils
- is identified in the school rules as a banned item for which a search can be carried out
- is evidence in relation to an offence

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

- make an assessment of how urgent the search is, and consider the risk to other pupils and staff; if the search is not urgent, they will seek advice from the Executive Headteacher
- explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- seek the pupil's cooperation

6.11 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.

6.12 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
- undermine the safe environment of the school or disrupt teaching
- commit an offence

6.13 If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or 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.

6.14 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 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

6.15 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 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
    - the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

6.16 Any searching of pupils will be carried out in line with:

- the DfE's latest guidance on searching, screening and confiscation
- the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- the school's Behaviour Policy

6.17 Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the federation's Complaints Procedure.

Artificial Intelligence

6.18 Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents may be familiar with generative chatbots such as ChatGPT and Google Bard.

6.19 The federation recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others e.g. in the form of 'deep fakes', where AI is used to create images, audio or video hoaxes that look real.

6.20 We will treat any use of AI to bully pupils in line with the federation's Anti-Bullying Policy.

6.21 Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the federation.

7 Acceptable use of the internet in school

7.1 All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the federation's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the federation's terms on acceptable use if relevant.

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

7.3 We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

7.4 More information is set out in our ICT and Internet Acceptable Use Policy.

8 Pupils using mobile devices in school

8.1 Middle school pupils are encouraged not to bring personal devices to school, but where this is deemed necessary by parents then pupils are responsible for handing in

their device at the beginning of the day and then collecting it at the end of the day; use during the day is not permitted.

8.2 ACHS students should ensure that personal mobile phones and personal devices are kept in a secure place, switched off and/or kept out of sight during lessons and while moving between lessons. The use of personal mobile phones or devices during non-formal school times is permitted in the yard and dining hall.

8.3 Mobile phones or personal devices will not be used by ACHS students during lessons or formal school time, unless as part of an approved and directed curriculum based activity with consent from a member of staff. If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.

8.4 If a pupil needs to contact their parents/carers they will be allowed to use a school telephone. Parents/carers are advised not to contact their child via their mobile phone during the school day, but to contact the school office in the first instance; exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by a member of the Senior Leadership Team.

8.5 Any use of mobile devices in school by pupils must be in line with the federation's ICT and Internet Acceptable Use Policy. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school's Behaviour Policy, which may result in the confiscation of their device.

9 Staff using work devices outside school

9.1 All staff members are expected to take appropriate steps to ensure their work devices remain secure in line with the federation's ICT and Internet Acceptable use Policy.

9.2 Work devices must be used solely for work activities and must not be used in any way which would violate the terms of the federation's ICT and Internet Acceptable use Policy.

9.3 If staff have any concerns over the security of their device, they must seek advice from the Business Manager - ICT and Infrastructure.

10 How the federation will respond to issues of misuse

10.1 Where a pupil misuses the federation's ICT systems or internet, we will follow the procedures set out in the school's Behaviour Policy and federation's ICT and Internet Acceptable Use Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

10.2 Where a staff member misuses the federation's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the federation's Disciplinary Policy and Code of Conduct for Staff and Volunteers. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

10.3 The federation will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11 Training

11.1 All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyberbullying and the risks of online radicalisation.

11.2 All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

11.3 By way of this training, all staff will be made aware that:

- technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- children can abuse their peers online through:
    - abusive, harassing, and misogynistic messages
    - non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - sharing of abusive images and pornography, to those who don't want to receive such content
- physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

11.4 Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

11.5 The DSLs and deputies will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

11.6 Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

11.7 Volunteers will receive appropriate training and updates, if applicable.

11.8 More information about safeguarding training is set out in the federation's Child Protection and Policy.

Appendix A: Online safety contacts and references

Local support and guidance

- Northumberland County Council Education Safeguarding Team: http://www.northumberland.gov.uk/Children/Safeguarding.aspx
- Northumberland County Council Local Authority Designated Officer (LADO): lado@northumberland.gov.uk or 01670 623979
- Northumbria Police: http://www.northumbria.police.uk/ or http://www.northumbria.police.uk/esafety; in an emergency (a life is in danger or a crime in progress) dial 999, or for other non-urgent enquiries dial 101
- Northumberland Safeguarding Children Board (NSCB): http://www.northumberland.gov.uk/Children/Safeguarding/Info.aspx

National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- BBC WebWise: www.bbc.co.uk/webwise
- CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
- ChildLine: www.childline.org.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- Know the Net: www.knowthenet.org.uk
- Net Aware: www.net-aware.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
- Parent Port: www.parentport.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/
- Virtual Global Taskforce: www.virtualglobaltaskforce.com
- UK Safer Internet Centre: www.saferinternet.org.uk
- 360 Safe Self-Review tool for schools: https://360safe.org.uk/
- Online Compass (self review tool for other settings): www.onlinecompass.org.uk