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	January 2020

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

1   Overview

1.1   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.

1.2   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.

1.3   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   Scope

2.1   The purpose of this policy is to:

- clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that the federation is a safe and secure environment
- safeguard and protect all members of the federation's community online
- raise awareness amongst all members of the federation's community regarding the potential risks as well as benefits of technology
- to enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology
- identify clear procedures to use when responding to online safety concerns that are known by all members of the community

2.2   The policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with federation issued devices for use off-site, such as laptops, tablets or mobile phones.

2.3   The policy applies to governors, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the federation (collectively referred to as 'staff' in this policy), as well as children and parents/carers.

2.4   This policy must be read in conjunction with other relevant federation policies including (but not limited to) the Child Protection, Anti-Bullying, Behaviour, Data Protection, and Acceptable Use by Staff policies.

3   Roles and responsibilities

Key personnel

The designated safeguarding leads (DSL) for child protection are Mr Graham Scott (ACHS/WMS) and Mrs Stephanie Lindley (SSMS)

Contact details: gscott@astleyhigh.org (0191 2371505 x207) /
stephanie.lindley@seatonsluice.northumberland.sch.uk (0191 2370629)

The deputy designated persons for child protection are Mr Jon Souter (ACHS/WMS), Mrs Karen McSparron (SSMS) and Mrs Kellyann Cook (SSMS)

Contact details: jon.souter@whytrig.northumberland.sch.uk (0191 2371402) /
karen.mcsparron@seatonsluice.northumberland.sch.uk (0191 2370629) /
kellyann.cook@seatonsluice.northumberland.sch.uk (0191 2370629)

The nominated child protection governor is Mrs Susan Dungworth

Contact details: sdungworth@astleyhigh.org

The Executive Headteacher is Mr John Barnes

Contact details: jbarnes@astleyhigh.org (0191 2371505 x230)

3.1   The key responsibilities of the **Senior Leadership Team** are:

- developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the federation community
- ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture
- supporting the Designated Safeguarding Lead (DSL) and Designated Child Protection Lead (DCPL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities
- ensuring that the Designated Safeguarding Lead (DSL) and Designated Child Protection Lead (DCPL) work effectively with the online safety lead
- ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use by Staff policy which covers appropriate professional conduct and use of technology
- ensuring that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material
- working with and supporting technical staff in monitoring the safety and security of the federation's systems and networks and to ensure that the federation's network system is actively monitored
- ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications
- ensuring that online safety is embedded within a progressive curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours

- being aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate
- receiving and regularly reviewing online safeguarding records and use them to inform and shape future practice
- ensuring there are robust reporting channels for the federation's community to access regarding online safety concerns, including internal, local & national support
- ensuring that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices
- ensuring a member of the Governing Body is identified with a lead responsibility for supporting online safety
- auditing and evaluating current online safety practice to identify strengths and areas for improvement
- enabling the local authority to carry out their "e-safety and ICT general controls" audit on a yearly basis for high schools (less frequently for middle schools)

3.2 The key responsibilities of the **Designated Safeguarding Lead** are:

- keeping up-to-date with current research, legislation and trends regarding online safety
- co-ordinating participation in local and national events to promote positive online behaviour e.g. Safer Internet Day
- ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches
- work with the federation's lead for data protection and data security to ensure that practice is in line with current legislation
- monitor the federation's online safety incidents to identify gaps/trends and use this data to update the federation's education response to reflect need
- report to the Senior Leadership Team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures
- liaising with the local authority and other local and national bodies, as appropriate
- working with the federation's Senior Leadership Team and IT & Technical Support Manager to review and update the Online Safety, Acceptable Use by Staff and other related policies on a regular basis (at least annually) with stakeholder input
- ensuring that online safety is integrated with other appropriate school policies and procedures
- meet regularly with the governor with a lead responsibility for online safety

3.3 The key responsibilities of the **Designated Child Protection Lead** are:

- acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate
- maintaining a record of online safety concerns/incidents and actions taken as part of the schools' safeguarding recording structures and mechanisms
- keeping up-to-date with current research, legislation and trends regarding online safety

3.4 The key responsibilities for **all members of staff** are:

- contributing to the development of online safety policies
- reading and adhering to the federation's Acceptable Use by Staff policy
- taking responsibility for the security of the federation's systems and data

- having an awareness of a range of different online safety issues and how they may relate to the children in their care
- modelling good practice when using new and emerging technologies
- embedding online safety education in curriculum delivery wherever possible
- identifying individuals of concern and taking appropriate action by following federation safeguarding policies and procedures
- knowing when and how to escalate online safety issues, internally and externally
- being able to signpost to appropriate support available for online safety issues, internally and externally
- maintaining a professional level of conduct in their personal use of technology, both on and off site
- demonstrating an emphasis on positive learning opportunities
- taking personal responsibility for professional development in this area

3.5 In addition to the above, the key responsibilities for **staff managing the technical environment** are:

- providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised
- taking responsibility for the implementation of safe security of systems and data in partnership with the Senior Leadership Team
- ensuring that suitable access controls and encryption is implemented to protect personal and sensitive information held on federation-owned devices
- ensuring that the federation's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL
- ensuring that the use of the federation's network is regularly monitored and reporting any deliberate or accidental misuse to the Student Progress Leader (SPL), pastoral lead and/or DCPL
- reporting any breaches or concerns to the DCPL and Senior Leadership Team and together ensure that they are recorded and appropriate action is taken as advised
- developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure
- reporting any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues
- providing technical support and perspective to the DSL and Senior Leadership Team, especially in the development and implementation of appropriate online safety policies and procedures
- ensuring that the federation's ICT infrastructure is secure and not open to misuse or malicious attack
- ensuring that appropriate anti-virus software and system updates are installed and maintained on all machines and portable devices
- ensure that appropriately secure passwords are applied and enforced as required by the local authority's ICT Audit team

3.6 The key responsibilities of **children and young people** are:

- contributing to the development of online safety policies
- reading and adhering to the relevant acceptable use policies
- respecting the feelings and rights of others both on and offline
- seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues
- at a level that is appropriate to their individual age, ability and vulnerabilities:
  o taking responsibility for keeping themselves and others safe online

- o taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- o assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks

3.7 The key responsibilities of **parents and carers** are:

- reading the relevant acceptable use policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate
- discussing online safety issues with their children, supporting the federation in their online safety approaches, and reinforcing appropriate safe online behaviours at home
- role modelling safe and appropriate use of technology and social media
- identifying changes in behaviour that could indicate that their child is at risk of harm online
- seeking help and support from the federation, or other appropriate agencies, if they or their child encounters online problems or concerns
- using federation systems, such as learning platforms and other network resources, safely and appropriately
- taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies

4 Online communication and safer use of technology

Federation website

- The federation will ensure that information posted on its website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the school address, email and telephone number; staff or pupils' personal information will not be published.
- The Executive Headteacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The website will comply with the federation's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
- Pupils' work will be published with their permission or that of their parents/carers.
- The administrator accounts for the federation website will be safeguarded with an appropriately strong password.
- The federation will post information about safeguarding, including online safety, on the website for members of the community.

Publishing images and videos online

- The federation will ensure that all use of images and videos, including sharing online, are used in accordance with the federation's Data Protection policy.
- Written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

Email

- Pupils may only use federation email accounts for educational purposes.
- All members of staff are provided with a federation email address to use for any official communication.

- The use of personal email addresses by staff for any official federation business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted; spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains content which could be subject to GDPR (e.g. sensitive or personal information) will only be sent after consideration of the need or method of communication and then only sent using secure and encrypted email.
- Access to the federation's email systems will always take place in accordance with GDPR legislation and in line with the federation's Data Protection and other appropriate policies.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the federation's safeguarding files/records.
- Whole-class or group email addresses may be used for communication outside of the federation.
- Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.
- Federation email addresses and other official contact details will not be used for setting up personal social media accounts.
- Staff will ensure that a line manager is copied into any e-mail communication with a pupil or group of pupils.

Video conferencing and webcam use for educational purposes

- The federation acknowledges that video conferencing is a challenging activity with a wide range of learning benefits; preparation and evaluation are essential.
- All video conferencing equipment will be switched off when not in use and, where appropriate, not set to auto answer.
- Where appropriate, webcams on portable devices are to be disabled or covered with tape to ensure no accidental usage.
- Video conferencing contact details will not be posted publicly.
- Staff will ensure that external video conference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.
- Pupils will ask permission from a teacher before making or answering a video conference call or message.
- Video conferencing will be supervised appropriately for the pupils' age and ability.
- Parent/carers' consent will be obtained prior to children taking part in video conferencing activities.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Video conferencing with take place 1:many, and not 1:1 where students may become individually identified.
- Only key administrators will be given access to video conferencing administration areas or remote control pages.
- When recording a video conference lesson, written permission will be given by all sites and participants; the reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference, and recorded material will be stored securely.
- If third party materials are to be included, the federation will check that recording is acceptable to avoid infringing the third party intellectual property rights.

- The federation will establish dialogue with other conference participants before taking part in a video conference; if it is a non-school site, the federation will check that they are delivering material that is appropriate for the class.

Appropriate and safe classroom use of the internet and any associated devices

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum; see specific curriculum policies for further information.
- Federation internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff should be aware that they cannot rely on filtering alone to safeguard children and supervision; classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability.
- Key Stage 2 pupils will be supervised; pupils will use age-appropriate online tools and online activities will be teacher-directed where necessary - children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
- Key Stage 3, 4 and 5 pupils will be appropriately supervised when using technology, according to their ability and understanding.
- All federation owned devices will be used in accordance with the federation's Acceptable Use by Staff policy and with appropriate safety and security measures in place; the federation will use e-safety software on all devices alongside filtering software.
- Members of staff will always evaluate websites, tools and apps fully before use with pupils in the classroom or suggesting websites for use at home.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Federation staff will ensure that the use of internet-derived materials by staff and pupils complies with copyright law and will acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a federation requirement across the curriculum.
- The federation will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

Federation learning platforms/portals/gateways

- The Senior Leadership Team and staff will regularly monitor the usage of learning platforms in all areas, in particular message and communication tools and publishing facilities.
- Pupils and staff will be advised about acceptable conduct and use when using a learning platform.
- Only members of the current pupil, parent/carers and staff community will have access to a learning platform.
- All users will be mindful of copyright issues and will only upload appropriate content onto a learning platform.
- When pupils leave the school their account or rights to specific school areas will be disabled.

- When staff leave the school their account or rights to specific school areas will be suspended in the first instance to ascertain the need for materials from the account to be shared with colleagues before being deleted.
- Any concerns about content on a learning platform will be recorded and dealt with in the following ways:
  o The user will be asked to remove any material deemed to be inappropriate or offensive.
  o The material will be removed by the site administrator if the user does not comply.
  o Access to a learning platform for the user may be suspended.
  o The user will need to discuss the issues with a member of the Senior Leadership Team before reinstatement.
  o A pupil's parent/carer may be informed.
- A visitor may be invited onto a learning platform by a member of the Senior Leadership Team; in this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff; this may be given to the pupil to fulfil a specific aim and may have a limited time frame.

5   Social media

General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of the federation community and exist in order to safeguard both the federation and the wider community, on and offline.
- Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chat rooms, instant messenger and many others.
- All members of the federation community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the federation community.
- All members of the federation community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The federation will control pupil and staff access to social media and social networking sites whilst on site and when using federation provided devices and systems.
- The use of social networking applications during school hours for personal use is not permitted.
- Inappropriate or excessive use of social media during school hours or whilst using federation devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of the federation community on social media sites should be reported to the Senior Leadership Team and will be managed in accordance with the federation's Child Protection and other relevant policies.
- Any policy breaches may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed; action taken will be in accordance with the federation's Child Protection and other relevant policies.

Official use of social media

- The federation's official social media channels are:
    - o https://twitter.com/seatonvalleyfed
    - o https://facebook.com/SeatonValleyFed (tbc)
    - o https://facebook.com/astleyhigh
    - o https://twitter.com/astleyhigh
    - o https://twitter.com/AstleyPE
    - o https://twitter.com/astley_maths
    - o https://twitter.com/WhytrigMS
    - o https://twitter.com/ssmssport
- Official use of social media channels by the federation will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official social media channels will only be created when authorised by a member of the Senior Leadership Team.
- The Executive Headteacher will take overall responsibility for the official use of social media sites as communication tools and will ensure that information is accurate and appropriate.
- Staff will use federation provided email addresses to register for and manage any official approved social media channels.
- Members of staff running official social media channels will sign a specific Acceptable Use by Staff policy statement to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including GDPR, the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998 or similar duty to protect private information, and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with the federation's Child Protection, Anti-Bullying and other relevant policies.
- Images or videos of children will only be shared on official social media sites/channels in accordance with the federation's Data Protection policy and after checking the appropriate parental permissions are in place to do so.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. with secure passwords), and where possible and appropriate, run and/or linked to from the federation's website and with written approval from the Senior Leadership Team.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Public communications on behalf of the federation will, where possible, be read and agreed by a member of the Senior Leadership Team.
- Official social media channels will link back to the federation's website and/or Acceptable Use by Staff policy to demonstrate that the account is official.
- The federation will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff official use of social media

● If members of staff are participating in online activity in their capacity as an employee of the federation, then they are requested to be professional at all times and to be aware that they are an ambassador for the federation.
● Staff using social media officially will disclose their official role but always make it clear that they do not necessarily speak on behalf of the federation.
● Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
● Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
● Staff must ensure that any image posted on any official social media channel has appropriate written parental consent.
● Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the federation unless they are authorised to do so.
● Staff using social media officially will not disclose names and personal details of pupils.
● Staff using social media officially will inform their line manager, the Designated Child Protection Lead and the Executive Headteacher of any concerns such as criticism or inappropriate content posted online.
● Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.
● Staff using social media officially will sign the federation's Social Media Acceptable Use policy.

Staff personal use of social media

● The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
● Safe and professional behaviour will be outlined for all members of staff (including volunteers) within the federation's Acceptable Use by Staff policy.
● Staff personal use of social media must not be undertaken during working time.
● All members of staff are advised not to communicate with or add as 'friends' any current or past children/pupils or current or past pupils' family members via any personal social media sites, applications or profiles; any pre-existing relationships or exceptions that may compromise this will be discussed with the Designated Child Protection Lead and/or the Executive Headteacher.
● If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
● All communication between staff and members of the federation community on school business will take place via official approved communication channels.
● Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior written approval has been given by the Executive Headteacher.
● Any communication from pupils/parents received on personal social media accounts will be reported to the school's Designated Child Protection Lead.

- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues, the federation etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites; this includes being aware of location sharing services, setting the privacy levels of personal sites as strictly as possible, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to 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 and is in accordance with relevant federation policies (e.g. Code of Conduct, Child Protection, Acceptable Use by Staff, Data Protection etc.) and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online; advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the federation.
- Members of staff are encouraged not to identify themselves as employees of the federation on their personal social networking accounts; this is to prevent information on these sites from being linked with the federation and also to safeguard the privacy of staff members and the wider community.
- Members of staff will ensure that they do not represent their personal views as that of the federation on social media.
- Federation email addresses will not be used for setting up personal social media accounts.
- Personal social media accounts, including email addresses, will not be used for setting up any accounts relating to the federation.
- The federation acknowledges that some members of staff live within the local community so have a conflict between some of the principles outlined above and the ability to interact as a member of the local community within a social networking environment; this policy should be read in conjunction with the Social Networking policy and staff should conduct themselves in a professional manner so as not to bring themselves or the federation into disrepute.

Pupils' use of social media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and/or their location; examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and secure passwords, deny access to unknown

individuals and be supported in learning how to block and report unwanted communications.

- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- Any official social media activity involving pupils will be moderated by the school where possible.
- As the federation is aware that many popular social media sites state that they are not for children under the age of 13, we will not create accounts within school for children under this age.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with the federation's Anti-Bullying, Behaviour and other relevant policies.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers via the Student Progress Leader, pastoral lead or Head of School, particularly when concerning any underage use of social media sites.

6   Use of personal devices and mobile phones

Rationale

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults requires all members of the federation community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The federation recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.
- The use of mobile phones and other personal devices by young people and adults will be decided by the federation and is covered in appropriate policies, including the federation's Acceptable Use policy.

Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and appropriate federation policies.
- Electronic devices of all kinds that are brought on site are the responsibility of the user at all times; the federation accepts no responsibility for the loss, theft or damage of such items, nor will the federation accept responsibility for any adverse health effects caused by any such devices, either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with in accordance with the Behaviour Policy.
- Members of staff will be issued with a work phone number and email address where contact with pupils or parents/carers is required.

- All members of the federation community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of the federation community will be advised to use passwords and PINs to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen; passwords and PINs should be kept confidential.
- Mobile phones and personal devices should not be shared.
- All members of the federation community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the federation's policies.
- Federation mobile phones and devices must always be used in accordance with the Acceptable Use by Staff policy and any other relevant policies.
- Federation mobile phones and devices used for communication with parents and pupils must be suitably protected via a complex password and not just a four digit PIN, and must only be accessed and used by members of staff.
- Staff accessing federation emails on a personal device must ensure the device is secured with a complex password and not just a four digit PIN, and that other family members do not have access to the device; if this is not possible then the use of a mail app is forbidden and federation email must only not be accessed via a browser which requires the staff member to login each time.

Pupils

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by children will take place in accordance with the Acceptable Use policy.
- ACHS students' personal mobile phones and personal devices will be kept in a secure place, switched off and/or kept out of sight during lessons and while moving between lessons.
- 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.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
- The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- 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 during non-formal school times is permitted in the yard and dining hall for ACHS students only.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office; exceptions may be permitted in

exceptional circumstances on a case-by-case basis and as approved by a member of the Senior Leadership Team.

- Pupils should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Mobile phones and personal devices, including smart wearable devices, must not be taken into examinations; pupils found in possession of a mobile phone, personal device or a smart wearable device during an exam will be reported to the appropriate examining body, which may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil breaches this policy then the phone or device will be confiscated and will be held in a secure place on the school site; mobile phones and devices will be released to parents/carers in accordance with each school's policy.
- Federation staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's behaviour or bullying policy or could contain youth produced sexual imagery (sexting); the phone or device may be searched by a member of the Senior Leadership Team with the consent of the pupil or parent/carer and content may be deleted or requested to be deleted.
- Appropriate searches of mobile phone or personal devices will only be carried out in accordance with this policy.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

Staff

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity; any pre-existing relationships which could compromise this should be discussed with the Executive Headteacher.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law (e.g. data protection) and the federation's Acceptable Use by Staff and other relevant policies and procedures.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Senior Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches this policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.

- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to in accordance with the relevant federation policies.

Visitors

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the federation's Acceptable Use policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the federation's Data Protection policy.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Child Protection Lead of any breaches of use by visitors.

7   Policy decisions

Reducing online risks

- The federation is aware that the internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the Senior Leadership Team will ensure that appropriate risk assessments are carried out before use in schools is allowed.
- The federation will ensure that appropriate internet filtering software and network monitoring software (auditing keystrokes, network activity and behaviours) are in place to prevent staff and pupils from accessing unsuitable or illegal content.
- The federation will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a federation computer or device.
- The federation will audit technology use to establish if the Online Safety policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the federation's Senior Leadership Team and IT & Technical Support Manager.

Internet use throughout the wider federation community

- The federation will liaise with local organisations to establish a common approach to online safety.
- The federation will work with the local community's needs (including recognising cultural backgrounds, languages, religions and ethnicity) to ensure internet use is appropriate.
- The federation will provide an Acceptable Use policy for any guest/visitor who needs to access the federation's computer systems or internet on site.

Authorising internet access

- The federation will maintain a current record of all staff and pupils who are granted access to the federation's devices and systems.
- All staff, pupils and visitors will read and sign the Acceptable Use policy before using any federation resources.

- Parents will be informed that pupils will be provided with supervised internet access which is appropriate to their age and ability.
- Parents will be asked to read the Acceptable Use policy for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the community e.g. children with special education needs, the federation will make decisions based on the specific needs and understanding of the pupil(s).

8   Engagement and education approaches

Children and young people

- An online safety curriculum will be established and embedded throughout the three schools, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.
- Pupil input will be sought when writing and developing federation online safety policies and practices, including curriculum development and implementation.
- Pupils will be supported in reading and understanding the Acceptable Use policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Online safety will be included in the PSHE and ICT curriculums across the federation, as well as regular year group assembly presentations, which covers both safe school and home use.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum and within all subject areas.
- External support may be used to complement and support the federation's internal online safety education approaches.
- The federation will reward positive use of technology by pupils.

Children and young people considered to be vulnerable

- Some children may be considered to be more vulnerable online due to a range of factors.
- The federation will ensure that differentiated and ability appropriate online safety education is given, with input from specialist staff as appropriate e.g. SENDCo.

Staff

- The Online Safety policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that all internet traffic can be monitored and traced to the individual user, and that discretion and professional conduct is essential when using federation systems and devices.
- Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular (at least annual) basis.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within federation; civil, legal or

disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

- Members of staff with a responsibility for managing filtering systems or monitoring ICT use will be supervised by the Senior Leadership Team and IT & Technical Support Manager, and will have clear procedures for reporting issues or concerns.
- The federation will highlight useful online tools which staff should use according to the age and ability of the pupils.

Parents and carers

- The federation recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats; parents' attention will be drawn to the federation's Online Safety policy and expectations in newsletters and on the federation website.
- A partnership approach to online safety at home and at school with parents will be encouraged; this may include offering specific sessions with demonstrations and suggestions for safe home internet use, or highlighting online safety at other well attended events e.g. parents' evenings.
- Parents will be encouraged to read the school's Acceptable Use policy for pupils and discuss its implications with their children.
- Parents will be encouraged to role model positive behaviour for their children online.

9   Information systems

Managing personal data online

- Personal data will be recorded, processed, transferred and made available in accordance with GDPR.
- Full information regarding the schools' approach to data protection and information governance can be found in the federation's Data Protection Policy.

Security and management of information systems

- The security of the federation's information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus and/or malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the federation networks will be regularly checked.
- The IT & Technical Support Manager will review system capacity on a regular basis.

- The appropriate use of user logins and passwords to access the federation's networks will be enforced for all users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.

Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- All members of staff will have their own unique username and private passwords to access federation systems.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- We require staff and pupils to use strong passwords for access into our system.
- We require staff and pupils to regularly change their passwords in accordance with the local authority's IT Audit advice.

Filtering and monitoring

- The governors will ensure that the federation has age and ability appropriate filtering and monitoring in place whilst using federation devices and systems to limit children's exposure to online risks.
- The federation's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- All monitoring of federation owned/provided systems will take place to safeguard members of the community.
- All users will be informed that use of federation systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The federation uses educational filtered secure broadband connectivity which is appropriate to the age and requirement of our pupils.
- The federation uses appropriate filtering systems which block sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The federation will work with the local authority and its broadband/filtering provider to ensure that the filtering policy is continually reviewed.
- The federation will have a clear procedure for reporting breaches of filtering which all members of the federation community (all staff and all pupils) will be made aware of.
- If staff or pupils discover unsuitable sites, the URL will be reported to the school's Designated Child Protection Lead and the federation's IT & Technical Support Manager, and will then be recorded and escalated as appropriate.
- The federation's filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the federation's filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- All changes to the school filtering policy will be logged and recorded.

- The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported immediately to appropriate agencies such as IWF, Police or CEOP.

Applications (apps) used to record children's progress

- The Executive Headteacher is ultimately responsible for the security of any data or images held of children.
- Apps/systems which store personal data will be risk assessed prior to use.
- Only federation issued devices will be used for apps that record and store children's personal details, attainment or photographs; personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- Parents will be informed of the federation's expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

10 Responding to online incidents and safeguarding concerns

General

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc.; this will be highlighted within staff training and educational approaches for pupils.
- All members of the federation community will be informed about the procedure for reporting online safety concerns, such as breaches of filtering, sexting, cyber bullying, illegal content etc.
- The Designated Child Protection Lead (DCPL) will be informed of any online safety incidents involving child protection concerns, which will then be recorded.
- The DCPL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Northumberland Safeguarding Children Board (NSCB) thresholds and procedures.
- Complaints about internet misuse will be dealt with under the federation's Complaints Procedure.
- Complaints about online/cyber bullying will be dealt with under the federation's Anti-Bullying Policy.
- Any complaint about staff misuse will be referred to the Executive Headteacher.
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the federation's Complaints Procedure.
- Staff will be informed of the federation's Whistleblowing Policy.
- All members of the federation's community will need to be aware of the importance of confidentiality and the need to follow the official federation procedures for reporting concerns.

- All members of the federation community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the federation's community.
- The federation will manage online safety incidents in accordance with the federation's Disciplinary Procedure or Behaviour Policy as appropriate.
- The federation will inform parents/carers of any incidents of concern as and when required.
- After any investigations are completed, the federation will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern, or fear that illegal activity has taken place or is taking place, then the school will contact the Northumberland Education Safeguarding Team, or Northumbria Police via 101 or 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Northumbria Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Northumberland Education Safeguarding Team.
- If an incident of concern needs to be passed beyond the federation community, then the concern will be escalated to the Northumberland Education Safeguarding Team to communicate to other schools in Northumberland.
- Parents and children will need to work in partnership with federation schools to resolve issues.

Youth produced sexual imagery or "sexting"

- The federation ensures that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").
- The federation will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- The federation views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Child Protection Lead (DCPL).
- The federation will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.
- If the federation is made aware of an incident involving creating youth produced sexual imagery the federation will:
  - act in accordance with the federation's Child Protection Policy and the relevant Northumberland Safeguarding Children Board procedures.
  - immediately notify the DCPL.
  - store the device securely.
  - carry out a risk assessment in relation to the child(ren) involved.
  - consider the vulnerabilities of child(ren) involved, including carrying out relevant checks with other agencies.
  - make a referral to children's social care and/or the police (as needed/appropriate).

- put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- implement appropriate sanctions in accordance with the federation's Behaviour Policy but taking care not to further traumatise victims where possible.
- review the handling of any incidents to ensure that the federation is implementing best practice and the leadership team will review and update any management procedures where necessary.
- inform parents/carers about the incident and how it is being managed.
- The federation 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 (in these cases the image will only be viewed by the DCPL).
- The federation will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the federation's network or devices then the federation will take action to block access to all users and isolate the image.
- The federation will take action regarding creating youth produced sexual imagery, regardless of the use of federation equipment or personal equipment, both on and off the premises.
- The federation will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Online child sexual abuse and exploitation

- The federation will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The federation will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- The federation views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Child Protection Lead (DCPL).
- If the federation is unclear if a criminal offence has been committed then the DCPL will obtain advice immediately through the Northumberland Education Safeguarding Team and/or Northumbria Police.
- If the federation is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the Northumberland Safeguarding Children Board by the DCPL.
- If the federation is made aware of an incident involving online child sexual abuse of a child then the federation will:
  - act in accordance with the federation's child protection and safeguarding policy and the relevant Northumberland Safeguarding Children Board procedures.
  - immediately notify the DCPL.
  - store any devices involved securely.

- immediately inform Northumbria police via 101 (using 999 if a child is at immediate risk).
- where appropriate, involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form at www.ceop.police.uk/safety-centre/
- carry out a risk assessment which considers any vulnerabilities of pupil(s) involved, including carrying out relevant checks with other agencies.
- make a referral to children's social care (if needed/appropriate).
- put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- inform parents/carers about the incident and how it is being managed.
- review the handling of any incidents to ensure that the federation is implementing best practice and that the Senior Leadership Team review and update any management procedures where necessary.
- The federation will take action regarding online child sexual abuse regardless of the use of federation equipment or personal equipment, both on and off the federation's premises.
- The federation will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted then the federation will seek support from the Northumberland Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.
- The federation will ensure that the Click CEOP report button is visible and available to pupils where current web hosting allows.

Indecent images of children

- The federation will ensure that all members of the community are made aware of the criminal nature of indecent images of children including the possible consequences.
- The federation will take action regarding indecent images of children regardless of the use of federation equipment or personal equipment, both on and off the premises.
- The federation will take action to prevent accidental access to indecent images of children e.g. using an internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and implementing appropriate web filtering, firewalls and anti-spam software.
- If the federation is unclear if a criminal offence has been committed then the Designated Child Protection Lead (DCPL) will obtain advice immediately through the Northumberland Education Safeguarding Team and/or Northumbria Police.
- If the federation is made aware of indecent images of children then the federation will:
  - act in accordance with the federation's Child Protection Policy and the relevant Northumberland Safeguarding Children Board procedures.
  - immediately notify the school's DCPL.
  - store any devices involved securely.
  - immediately inform appropriate organisations e.g. the IWF, Northumbria Police via 101 (using 999 if a child is at immediate risk) and/or the Local

Authority Designated Officer (if there is an allegation against a member of staff or a volunteer).

- If the federation is made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the federation will:
    o ensure that the DCPL is informed.
    o ensure that the URLs (webpage addresses) which contain the suspect images are reported to the federation's IT & Technical Support Manager and the Internet Watch Foundation via www.iwf.org.uk.
    o ensure that any copies that exist of the image, for example in emails, are deleted.
- If the federation is made aware that indecent images of children have been found on the federation's electronic devices then the federation will:
    o ensure that the DCPL is informed.
    o ensure that the URLs (webpage addresses) which contain the suspect images are reported to the federation's IT & Technical Support Manager and the Internet Watch Foundation via www.iwf.org.uk.
    o take control of the devices to ensure the imagery is not deleted until any investigation by the DCPL or police has concluded
    o ensure that any copies that exist of the image, for example in emails, are deleted (once DCPL/police investigations have concluded).
    o inform the police via 101 (using 999 if there is an immediate risk of harm) and children's social services (as appropriate).
    o only store copies of images at the request of the police; this will be done securely so that no one else has access to them and all other copies are deleted.
- If the federation is made aware that a member of staff or volunteer is found in possession of indecent images of children on their electronic device provided by the federation, then the federation will:
    o ensure that the DCPL or another member of staff is informed in accordance with the federation's Procedure for Dealing with Allegations of Abuse.
    o contact the police regarding the images and quarantine any devices involved until police advice has been sought.
    o inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the federation's Procedure for Dealing with Allegations of Abuse.
    o follow the appropriate federation procedures regarding allegations of misconduct.

Radicalisation and extremism online

- The federation will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the DCPL will be informed immediately and action will be taken in line with the federation's Child Protection Policy.

- Online hate content directed towards or posted by specific members of the community will be responded to in line with the federation's Behaviour and other relevant policies.
- If the federation is unclear if a criminal offence has been committed then the DCPL will obtain advice immediately via the Northumberland Education Safeguarding Team and/or Northumbria Police.

Cyber bullying

- Cyber bullying, along with all other forms of bullying, of any member of the federation's community will not be tolerated; full details are set out in the federation's Anti-Bullying and Behaviour policies.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the federation community affected by online bullying.
- If the federation is unclear if a criminal offence has been committed then the DCPL will obtain advice immediately through the Northumberland Education Safeguarding Team and/or Northumbria Police.
- Pupils, staff and parents/carers will be advised to keep a record of cyber bullying as evidence.
- The federation will take steps to identify the bully where possible and appropriate; this may include examining federation system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the federation to support the approach to cyber bullying and the federation's e-safety ethos.
- Sanctions for those involved in online or cyber bullying may include:
  - asking those involved to remove any material deemed to be inappropriate or offensive.
  - contacting a service provider to remove content, if those involved refuse to or are unable to delete content.
  - suspending school internet access for the user for a period of time.
- Other sanctions for pupils and staff may also be used in accordance with the federation's Anti-Bullying, Behaviour or Acceptable Use by Staff policies.
- Parent/carers of pupils involved in online bullying will be informed.
- The police will be contacted if a criminal offence is suspected.

Online hate

- Online hate at The Seaton Valley Federation will not be tolerated; full details are set out in the federation's Anti-Bullying and Behaviour policies.
- All incidents of online hate reported to the federation will be recorded.
- If the federation is unclear if a criminal offence has been committed then the Designated Child Protection Lead will obtain advice immediately through the Northumberland Education Safeguarding Team and/or Northumbria Police.
- All members of the community will be advised to report online hate in accordance with relevant federation policies.
- The police will be contacted if a criminal offence is suspected.

11 Online safety contacts and references

<u>Local support and guidance</u>

- 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

<u>National Links and Resources</u>

- 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/
- Think U Know: www.thinkuknow.co.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