



## **Introduction**

This online safety policy has been written by Seaham Trinity, involving staff, learners and parents/carers, building on the Durham County Council online safety policy template, with specialist advice and input as required.

It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2019, Early Years and Foundation Stage 2017 'Working Together to Safeguard Children' 2018 and the Durham Safeguarding Children's Partnership procedures.

It is recommended that pupils, parents and staff are included in the development of a school e-Safety policy as well as the Governing Body. This policy has been written to reflect the schools own decisions on balancing educational benefit with potential risks. It should be used in conjunction with policies relating to curriculum, data protection, anti-bullying, safeguarding children, security and home-school agreements.

The Headteacher has identified himself (Ray Bushby) and Kim Clayton as the online safety co-ordinators. This policy has been prepared by the e-safety co-ordinator and has been agreed by the Headteacher and Governing Body.

## **Rationale**

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

## **Scope**

Seaham Trinity believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online. We identify that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. Seaham Trinity believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online. This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy), as well as learners, parents and carers. This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

## **Aims**

The purpose of Seaham Trinity's online safety policy is to:

- Safeguard and protect all members of Seaham Trinity community online
- Identify approaches to educate and raise awareness of online safety throughout the community
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns.
- Seaham Trinity identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

**Content:** being exposed to illegal, inappropriate or harmful material

**Contact:** being subjected to harmful online interaction with other users

**Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

### **Links with other policies and practices**

This policy links with several other policies, practices and action plans including: (Amend list as appropriate)

- Anti-bullying policy
- Acceptable Use Policies (AUP) and/or the Code of Conduct/Staff Behaviour policy
- Behaviour and Discipline policy
- Child Protection/Safeguarding policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data Protection (GDPR)
- Image Use policy

### **Monitoring and Review**

Technology in this area evolves and changes rapidly. Seaham Trinity will review this policy at least annually.

- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the headteacher/ DSL will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

### **Roles and Responsibilities**

The Designated Safeguarding Lead (DSL), Kim Clayton, has lead responsibility for online safety. Whilst activities of the designated safeguarding lead may be delegated to the Computing co ordinator, Victoria Light, but overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL. Seaham Trinity recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

#### **The leadership and management team will:**

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

**The Designated Safeguarding Lead (DSL) will:**

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant up to date knowledge required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the setting's management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety.

**It is the responsibility of all members of staff to:**

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

**It is the responsibility of staff managing the technical environment to:**

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

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

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others, both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

**It is the responsibility of parents and carers to:**

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement and/or acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately. (If in place)
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

**Education and Engagement Approaches**

**Education and engagement with learners**

The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

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

- Displaying acceptable use posters in all rooms with internet access.
- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

### **Vulnerable Learners**

Seaham Trinity recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to, children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.

When implementing an appropriate online safety policy and curriculum, Seaham Trinity will seek input from specialist staff as appropriate, including the SENCO (Kerry Robinson) and Child in Care Designated Teacher (Kim Clayton).

### **Training and engagement with staff**

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates (all staff complete an Online Safety Staff CPD course from the Online Safety Alliance annually and new staff complete this course when they start).

This will cover the potential risks posed to learners (Content, Contact and Conduct), as well as our professional practice expectations.

- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.

- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

### **Awareness and engagement with parents and carers**

Seaham Trinity recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

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

- Providing information and guidance on online safety in a variety of formats.
- This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
- Requiring them to read our acceptable use policies and discuss the implications with their children.

### **Reducing Online Risks**

Seaham Trinity recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.

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

### **Safer Use of Technology**

#### **Classroom Use**

Seaham Trinity uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices

- Internet which may include search engines and educational websites
- Learning platform/intranet
- Email
- Digital cameras, web cams and video cameras.

All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Seaham Trinity uses age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community. We use the Smoothwall filtering system which ensures that when using Google it is automatically set to safe search. This reduces but does not eliminate the risk of links to inappropriate content. We also have Kiddle set as the default homepage for the pupils to use as their search engine which brings up more age appropriate websites.
- We will ensure that the use of internet-derived materials, by staff and learners, complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.

### **Early Years Foundation Stage and Key Stage 1**

Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners' age and ability.

### **Key Stage 2**

- Learners will use age-appropriate search engines and online tools.
- Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners' age and ability.

### **Managing Internet Access**

All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

### **Filtering and Monitoring**

#### **Decision Making**

- Seaham Trinity governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learners' exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

## **Filtering**

- Education broadband connectivity is provided through Durham County Council.
- We use Smoothwall which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- All school devices should be connected to a filtered feed. If a school device needs access to additional content, for instance to manage official social media, the filter settings for that device or user should be modified to allow access to that content.
- We work with ICTSS to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
  - Turn off monitor/screen and report the concern immediate to a member of staff.
  - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
  - The breach will be recorded and escalated as appropriate.
  - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the UK Safer Internet Centre, Durham Police or CEOP.

## **Monitoring**

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
  - Physical monitoring (supervision), monitoring internet and web access (reviewing logfile information) and/or active/pro-active technology monitoring services).
- If a concern is identified via monitoring approaches we will:
  - DSL or deputy will respond in line with the child protection policy.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

## **Managing Personal Data Online**

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. Full information can be found in our Data Protection policy.

## **Security and Management of Information Systems**

- We take appropriate steps to ensure the security of our information systems, including: (Amend and add as appropriate)
  - Virus protection being updated regularly.



- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
- Specific user logins and passwords will be enforced for all but the youngest users (for KS2 pupils).
- All users are expected to log off or lock their screens/devices if systems are unattended.
- 

### **Password policy**

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From Year 3 all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
  - Use strong passwords for access into our system.
  - Change their passwords every year
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Not to login as another user at any time.

### **Managing the Safety of our Website**

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learners' personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

### **Publishing Images and Videos Online**

We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

### **Managing Email**

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
  - The forwarding of any chain messages/emails is not permitted.
  - Spam or junk mail will be blocked and reported to the email provider.

- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
  - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell (Ray Bushby HT or Kim Clayton DSL) if they receive offensive communication, and this will be recorded in our safeguarding files/records.
  - Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

### **Staff email**

- The use of personal email addresses by staff for any official setting business is not permitted.
  - All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

### **Learner email**

Learners will use provided email accounts for educational purposes.

- Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

### **Educational use of Videoconferencing and/or Webcams**

- Seaham Trinity recognise that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.
  - All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.
  - Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
  - Videoconferencing contact details will not be posted publicly.
  - Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.
  - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
  - Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

### **Users**

- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
- Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the learners age and ability. We ask that parents are present in the room during the video conferencing sessions for pupils of all ages.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.

- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

### **Content**

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third-party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

### **Management of Learning Platforms**

Seaham Trinity uses Microsoft Teams as its official learning platform for setting work and for communication. The school also uses Class Dojo for communication and publishing facilities.

- Leaders and staff will regularly monitor the usage of the Learning Platform (LPs), including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LPs.
- When staff and/or learners leave the setting, their account will be disabled or transferred to their new establishment.
- Learners and staff will be advised about acceptable conduct and use when using the LPs.
- All users will be mindful of copyright and will only upload appropriate content onto the LPs.
- Any concerns about content on the LPs will be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - If the user does not comply, the material will be removed by the site administrator.
  - Access to the LPs for the user may be suspended.
  - The user will need to discuss the issues with a member of leadership before reinstatement.
  - A learner's parents/carers may be informed.
  - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LPs by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

### **Management of Applications (apps) used to Record Children's Progress**

- We use Tapestry in the EYFS to track learners progress and share appropriate information with parents and carers. During remote learning, we also use 'Class Dojo' to set and mark children's work, we also leave feedback on their progress in this work which is also shared with parents.
- The headteacher/manager (Ray Bushby) is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and

that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

- To safeguard learners' data:
  - Only school issued devices will be used for apps that record and store learners' 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 learners' personal details, attainment or images.
  - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach in the event of loss or theft.
  - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
  - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

## **Social Media**

### Expectations

- The expectations regarding safe and responsible use of social media applies to all members of Seaham Trinity community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Seaham Trinity community are expected to engage in social media in a positive, safe and responsible manner.
- All members of Seaham Trinity 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.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site, these cannot be accessed on school devices as they are blocked using our filtering systems.
- The use of social media during setting hours for personal use is/is not permitted.
- Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Seaham Trinity community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

### **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) as part of our code of conduct/behaviour policy as part of acceptable use policy.

### Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
  - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
  - o Setting the privacy levels of their personal sites.
  - o Being aware of location sharing services.
  - o Opting out of public listings on social networking sites.
  - o Logging out of accounts after use.
  - o Keeping passwords safe and confidential.
  - o Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of Seaham Trinity on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- 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 our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

### **Communicating with learners and parents and carers**

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
  - Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputy) and/or the headteacher/manager.
  - If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the headteacher/manager.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

### **Learners' Personal Use of Social Media**

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.

- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore, we will not create accounts specifically for learners under this age.
- Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
  - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
  - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
  - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
  - To use safe passwords.
  - To use social media sites which are appropriate for their age and abilities.
  - How to block and report unwanted communications.
  - How to report concerns both within the setting and externally.

### **Official Use of Social Media**

- Seaham Trinity official social media channels are Facebook and Class Dojo.
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
  - The official use of social media as a communication tool has been formally risk assessed and approved by the headteacher/manager.
  - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
  - Staff use setting provided email addresses to register for and manage any official social media channels.
  - Official social media sites are suitably protected and, where possible, run and/or linked to/from our website.
  - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: anti-bullying, image/camera use, data protection, confidentiality and child protection.
  - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
  - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
  - Any official social media activity involving learners will be moderated possible.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We 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 expectations**

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
  - Sign our social media acceptable use policy.
  - Always be professional and aware they are an ambassador for the setting.
  - Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of the setting.
  - Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
  - Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
  - Ensure that they have appropriate consent before sharing images on the official social media channel.
  - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
  - Not engage with any direct or private messaging with current, or past, learners, parents and carers.
  - Inform their line manager, the DSL (or deputy) and/or the headteacher/manager of any concerns, such as criticism, inappropriate content or contact from learners.

## **Use of Personal Devices and Mobile Phones**

- Seaham Trinity recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

### **Expectations**

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
  - All members of Seaham Trinity community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
  - All members of Seaham Trinity community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the 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; any breaches will be dealt with as part of our behaviour policy.
- All members of Seaham Trinity community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.
- All members of Seaham Trinity community are reminded that taking covert images typically under clothing (Upskirting) is illegal and will be dealt with as part of the discipline policy.

## **Staff Use of Personal Devices and Mobile Phones**

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.
- Staff will be advised to:
  - Keep mobile phones and personal devices in a safe and secure place (List details e.g. locked in a locker/drawer) during lesson time.
  - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
  - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
  - Not use personal devices during teaching periods, unless verbal or written permission has been given by the headteacher/manager, such as in emergency circumstances.
  - Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are NOT permitted to use their own personal phones or devices for contacting learners or parents and carers.
  - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy) and/or headteacher/manager.
- Staff will not use personal devices:
  - To take photos or videos of learners and will only use work-provided equipment for this purpose.
  - Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy
  - 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, the police will be contacted.

## **Learners' Use of Personal Devices and Mobile Phones**

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Seaham Trinity expects learners' personal devices and mobile phones to be...
  - Handed in to the class teachers where they will be kept in a secure place, switched off, kept out of sight during lessons and while moving between lessons.
- If a learner needs to contact his/her parents or carers they will be allowed to use a setting phone.
  - Parents are advised to contact their child via the setting office.
- Mobile phones or personal devices will not be used by learners during lessons or formal educational time.
  - If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.
  - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
  - Searches of mobile phone or personal devices will only be carried out in accordance with our policy. (Appropriate for schools only and must link to appropriate policy. See [www.gov.uk/government/publications/searching-screening-and-confiscation](http://www.gov.uk/government/publications/searching-screening-and-confiscation))



- Learners' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/carer. Content may be deleted or requested to be deleted, if it contravenes our policies. (Appropriate for schools only and must link to appropriate policy. See [www.gov.uk/government/publications/searching-screening-and-confiscation](http://www.gov.uk/government/publications/searching-screening-and-confiscation))
- Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the day.
- If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

### **Visitors' Use of Personal Devices and Mobile Phones**

- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or headteacher/manager of any breaches our policy.

### **Officially provided mobile phones and devices**

- Members of staff will be issued with a work phone number and email address, where contact with learners or parents/carers is required.
- Setting mobile phones and devices will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff.
- Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.