E-Safety and Online ICT Policy

Approved by Governors: Spring 2019
Review Date: Spring 2020
Person Responsible: Deputy Headteacher
Key Details

Designated Safeguarding Lead (s): (Mark Foster, Deputy Headteacher)

Named Governor with lead responsibility: (Natalie Brown)

Date written: (November 2018)

Date agreed and ratified by Governing Body: (Month, Year)

Date of next review: (Month, Year)

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure.
Contents

1. Policy Aims .......................................................................................................................... 5
2. Policy Scope .......................................................................................................................... 5
   a. Links with other policies and practices ........................................................................... 5
3. Monitoring and Review ......................................................................................................... 5
4. Roles and Responsibilities .................................................................................................... 6
   a. The leadership and management team will: ................................................................. 6
   b. The Designated Safeguarding Lead (DSL) will: ......................................................... 7
   c. It is the responsibility of all members of staff to: ......................................................... 7
   d. It is the responsibility of staff managing the technical environment to: .................... 8
   e. It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to: ........................................................................ 8
   f. It is the responsibility of parents and carers to: ........................................................... 8
5. Education and Engagement Approaches ............................................................................ 9
   a. Education and engagement with learners ..................................................................... 9
   b. Vulnerable Learners ....................................................................................................... 9
   c. Training and engagement with staff ............................................................................. 10
   d. Awareness and engagement with parents and carers .................................................. 10
6. Reducing Online Risks ........................................................................................................ 11
7. Safer Use of Technology ...................................................................................................... 11
   a. Classroom Use ............................................................................................................... 11
   b. Managing Internet Access ............................................................................................. 12
   c. Filtering and Monitoring ............................................................................................... 12
   d. Managing Personal Data Online .................................................................................... 13
   e. Security and Management of Information Systems ....................................................... 13
   f. Password policy (if not covered in other policies) .......................................................... 14
   g. Managing the Safety of our Website .............................................................................. 14
   h. Publishing Images and Videos Online ........................................................................... 14
   i. Managing Email ............................................................................................................. 14
   j. Educational use of Videoconferencing and/or Webcams (Only include if used)............ 16
      k. Management of Learning Platforms (If used) ............................................................. 15
      l. Management of Applications (apps) used to Record Children’s Progress (If used) .... 16
8. Social Media ........................................................................................................................ 16
   a. Expectations ................................................................................................................... 16
   b. Staff Personal Use of Social Media .............................................................................. 17
   c. Learners Personal Use of Social Media ...................................................................... 18
   d. Official Use of Social Media (Only include if setting has official social media) .......... 19
9. Use of Personal Devices and Mobile Phones .................................................................... 20
   a. Expectations ................................................................................................................... 20
   b. Staff Use of Personal Devices and Mobile Phones ....................................................... 21

E-Safety and Online ICT Policy
Sedgefield Community College
E-Safety and Online ICT Policy
Sedgefield Community College

10. Responding to Online Safety Incidents and Concerns .......................................................... 23
   a. Concerns about Learners Welfare .................................................................................. 23
   b. Staff Misuse .................................................................................................................. 23
   c. Procedures for Responding to Specific Online Incidents or Concerns ................. 24

11. Useful Links for Educational Settings ............................................................................. 29

12. Staff and Student ICT Usage Agreements (Appendices) .......................................... 32
Sedgefield Community College Online Safety Policy

1. Policy Aims

- This online safety policy has been written by Sedgefield Community College, involving staff, learners and parents/carers, building on the Kent County Council/The Education People/Durham County Council online safety policy template, with specialist advice and input as required.
- The purpose of Sedgefield Community College’s online safety policy is to:
  - Safeguard and protect all members of the Sedgefield 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.
- Sedgefield Community College 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.

2. Policy Scope

- Sedgefield Community College 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.
- Sedgefield Community College identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Sedgefield Community College 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.

a. Links with other policies and practices

This policy links with several other policies, practices and action plans including Anti-bullying policy
- Anti-bullying policy
- Use of ICT and E-Safety Policy
- School Code of Conduct Policy
- Behaviour for Learning Policy
- Child Protection / Safeguarding policy
- Confidential Reporting / Whistleblowing policy
- Curriculum Policies, such as: Personal Social and Health Education (PSHE), Relationships and Sex Education (RSE)
- Data Protection
- Drugs Education Policy
- Photography and Digital Images policy
- Preventing Extremism and Radicalisation Policy
- School Drugs, Substance and Alcohol Misuse Policy

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. Sedgefield Community College 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 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.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL), Mark Foster, Deputy Headteacher has lead responsibility for online safety. **Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.**
- Sedgefield Community College recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

a. 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 code of conduct and Use of ICT 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.

b. The Designated Safeguarding Lead (DSL) will:

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

c. 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 Code of Conduct 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.

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

e. 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.

f. 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 responsible internet and computer use agreement.
• 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 FROG, and other network resources, safely and appropriately.
• Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

a. 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:
  o Ensuring education regarding safe and responsible use precedes internet access.
  o Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
  o Reinforcing online safety messages whenever technology or the internet is in use.
  o Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  o 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:
  o Displaying acceptable use posters in appropriate rooms.
  o Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  o Implementing appropriate peer education approaches through the Student Voice and Wellbeing Council.
  o Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
  o Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
  o Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

b. Vulnerable Learners

• Sedgefield Community College 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.

- Sedgefield Community College 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 Sedgefield Community College will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher.

c. Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
  - This will be completed during the annual safeguarding refresher training all staff receive each academic year. New staff will receive training during their induction programme.
  - 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.

d. Awareness and engagement with parents and carers

- Sedgefield Community College 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.
o Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- Sedgefield Community College recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
  o Regularly review the methods used to identify, assess and minimise online risks.
  o Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
  o Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
  o 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.

7. Safer Use of Technology

a. Classroom Use

- Sedgefield Community College uses a wide range of technology. This includes access to:
  o Computers, laptops, tablets and other digital devices
  o Internet which may include search engines and educational websites
  o Learning platform/intranet
  o Email
  o Games consoles and other games-based technologies
  o 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.
  o The Smoothwall filtering system is used to record and monitor the access to websites by students and staff. Only websites that are ‘white listed’ can be accessed during setting hours.
  o Airwatch is used to control the download of Apps onto tablet devices to a pre-agreed list.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
  o The Smoothwall filtering system used at Sedgefield Community College 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 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.
  o **Key Stage 3 and 4**
    ▪ Learners will be appropriately supervised when using technology, according to their ability and understanding.

b. **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.

c. **Filtering and Monitoring**

  i  **Decision Making**

   • Sedgefield Community College governors and senior leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner’s exposure to online risks.
   • The governors and senior 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.

  ii  **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.
   • We work with ICTSS to ensure that our filtering policy is continually reviewed.
   • If learners discover unsuitable sites, they will be required to:
     o Turn off monitor/screen and report the concern immediate to a member of staff.
     o 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.
     o The breach will be recorded and escalated as appropriate.
     o 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.

iii Monitoring
• We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
  o The duty Year Manager at the end of each day will run manual Smoothwall reports and highlight any concerns with the safeguarding team.
• If a concern is identified via monitoring approaches we will:
  o Investigate the concern in conjunction with the person identified, ICTSS and the DSL (or deputy)
• 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.

d. 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.
  o Full information can be found in our Data Protection policy.

e. Security and Management of Information Systems
• We take appropriate steps to ensure the security of our information systems, including:
  o Virus protection being updated regularly.
  o 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.
  o Not using portable media without specific permission; portable media will be checked by an anti-virus/malware scan before use.
  o Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  o Regularly checking files held on our network,
  o The appropriate use of user logins and passwords to access our network.
    ▪ Specific user logins and passwords will be enforced for all
  o All users are expected to log off or lock their screens/devices if systems are unattended.
  o Further information about technical environment safety and security can be found at:
    ▪ Appendix 1 Responsible Internet & Computer Use (Staff Agreement)
    ▪ Appendix 2 Responsible Internet & Computer Use (Student Agreement)
    ▪ Appendix 3 Parent’s Consent for Internet Access
    ▪ Appendix 4 Laptop / Tablet Usage Agreement (Staff)
    ▪ Appendix 5 Tablet device Responsible Usage Agreement (Student)
f. 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 7 users should log in with a username and a password set by the pupil.
- We require all users to:
  - Use strong passwords for access into our system. Minimum 12 characters including 2 special characters (Capital letters, numbers or symbols).
  - Change their passwords every 60 days.
  - 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.

g. 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 learner’s 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.

h. Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices, 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.

i. 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 Mark Foster, Deputy Headteacher 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.

i  Staff email
  o 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.
  o 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.

ii 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.

j. Management of Learning Platforms (If used)
  • Sedgefield Community College uses FROG as its official learning platform.
  • Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
  • Only current members of staff, learners and parents will have access to the LP.
  • 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 LP.
  • All users will be mindful of copyright and will only upload appropriate content onto the LP.
  • Any concerns about content on the LP 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 If the user does not comply, the material will be removed by the site administrator.
    o Access to the LP for the user may be suspended.
    o The user will need to discuss the issues with a member of leadership before reinstatement.
    o A learner’s parents/carers may be informed.
    o 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.

E-Safety and Online ICT Policy
Sedgefield Community College 15
• A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

k. Management of Applications (apps) used to Record Children’s Progress

• We use SIMs and SISRA to track learners progress and share appropriate information with parents and carers.
• The Headteacher, 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 learner’s data:
  o Only school issued devices will be used for apps that record and store learners’ personal details, attainment or photographs.
  o 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.
  o 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.
  o All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
  o 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.

8. Social Media

a. Expectations

• The expectations’ regarding safe and responsible use of social media applies to all members of the Sedgefield Community College 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 Sedgefield Community College community are expected to engage in social media in a positive, safe and responsible manner.
  o All members of the Sedgefield Community College 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.
  o The use of social media during setting hours for personal use is not permitted.
  o Access to the school official Twitter and Facebook accounts is permitted for educational purposes.
o 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 the Sedgefield Community College 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.

b. 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.
  o 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 Sedgefield Community College 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 with 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.
  - 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.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

**c. 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.
d. Official Use of Social Media

- Sedgefield Community College official social media channels are:
  - Twitter and Facebook.

- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
  o The official use of social media as a communication tool has been formally risk assessed and approved by the headteacher.
  o 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.
  o Staff use setting provided email addresses to register for and manage any official social media channels.
  o Official social media sites are suitably protected and, where possible, run and/or linked to/from our website.
  o 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.
  o 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.
  o Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
  o 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 professionals 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:
  o Sign our Responsible Internet & Computer Use acceptable use policy.
  o Always be professional and aware they are an ambassador for the setting.
  o Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of the setting.
  o 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 of any concerns, such as criticism, inappropriate content or contact from learners.

9. Use of Personal Devices and Mobile Phones

- Sedgefield Community College 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.

a. 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 the Sedgefield Community College 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 the Sedgefield Community College 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 and toilets.

- 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 the Sedgefield Community College 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.
b. 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:

- Appendix 1 Responsible Internet & Computer Use (Staff Agreement)
- Appendix 4 Laptop / Tablet Usage Agreement (Staff)
- Confidentiality, child protection, data security policies.

- Staff will be advised to
  - Keep mobile phones and personal devices in a safe and secure place 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 written permission has been given by the headteacher, 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.

- 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.

c. 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.
- Sedgefield Community College expects learners’ personal devices and mobile phones to be...
  - Kept in a secure place, switched off, kept out of sight whenever in the main buildings and at all times after 9.05am.
- If a learner needs to contact his/her parents or carers they will be allowed to use a Sedgefield Community College phone at student services.
Parents are advised to contact their child via the setting office; exceptions may be permitted on a case-by-case basis, as approved by the headteacher.

- Mobile phones or personal devices will not be used by learners during lessons or formal educational 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 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.

- Mobile phones and personal devices must not be taken into examinations.
  - Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

- If a learner breaches the policy, the phone or device will be confiscated and will be held in the school safe in a labelled envelope.
  - 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 Safeguarding policy.
  - 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.
  - Mobile phones and devices that have been confiscated will be released to parents or carers at the earliest opportunity.
  - 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.

d. 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 of any breaches our policy.

e. 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.

10. **Responding to Online Safety Incidents and Concerns**

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
  - Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Team or Durham Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or headteacher will speak with Durham Police first to ensure that potential investigations are not compromised.

a. **Concerns about Learners Welfare**

- The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.
  - The DSL (or deputy) will record these issues in line with our child protection policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the LSCB thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

b. **Staff Misuse**

- Any complaint about staff misuse will be referred to the headteacher, in accordance with the allegations policy.
- Any allegations regarding a member of staff’s online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.
c. Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children

- Sedgefield Community College recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
  - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- Sedgefield Community College recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Sedgefield Community College also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Sedgefield Community College will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
  - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
  - If content is contained on learners electronic devices, they will be managed in accordance with the DfE ‘searching screening and confiscation’ advice.
  - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
  - Implement appropriate sanctions in accordance with our behaviour policy.
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - If appropriate, make a referral to partner agencies, such as First Contact and/or the Police.
If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.

- If a criminal offence has been committed, the DSL (or deputy) will discuss this with Durham Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Youth Produced Sexual Imagery (\textquotedblleft Sexting\textquotedblright)

- Sedgefield Community College recognises youth produced sexual imagery (known as \textquotedblleft sexting\textquotedblright) as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCCIS guidance: \textit{\textquotedblleft Sexting in schools and colleges: responding to incidents and safeguarding young people\textquotedblright} and KSCB guidance: \textit{\textquotedblleft Responding to youth produced sexual imagery\textquotedblright}.
- Sedgefield Community College will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of \textquoteleft sexting\textquoteright by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
  - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
    - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
  - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
  - Act in accordance with our child protection policies and the relevant Durham LSCB procedures.
  - Ensure the DSL (or deputy) responds in line with the \textit{\textquotedblleft Sexting in schools and colleges: responding to incidents and safeguarding young people\textquotedblright} guidance.
  - Store the device securely.
If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.

- Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed. Additional resources are available on the Extranet for both Pupils and Parents.
- Make a referral to First Contact and/or the Police, as deemed appropriate in line with the UKCCIS: ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ guidance.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatis young people.
- Consider the deletion of images in accordance with the UKCCIS: ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ guidance.
  - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

d. Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- Sedgefield Community College will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Sedgefield Community College recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the ‘The Big Red Button! Keep Safe’ (Click CEOP) report button is visible and available to learners and other members of our community. This is accessible from the school website and the FROG learning platform.
If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
  o Act in accordance with our child protection policies and the relevant Durham LSCB procedures.
  o If appropriate, store any devices involved securely.
  o Make a referral to First Contact (if required/appropriate) and immediately inform Durham police via 101, or 999 if a child is at immediate risk.
  o Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
  o Inform parents/carers about the incident and how it is being managed.
  o Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
  o Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
  o Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the ‘The Big Red Button! Keep Safe’ (Click CEOP) report button: www.ceop.police.uk/safety-centre/

If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Durham or Durham Police.

If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Durham Police and/or Education Durham first to ensure that potential investigations are not compromised.

e. Indecent Images of Children (IIOC)

Sedgefield Community College will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Durham Police and/or the Education Safeguarding Team.

If made aware of IIOC, we will:
  o Act in accordance with our child protection policy and the relevant Durham LSCB procedures.
  o Store any devices involved securely.
If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and First Contact
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the headteacher is informed in line with our managing allegations against staff policy.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

f. Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Sedgefield Community College.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

g. Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Sedgefield Community College and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
• If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through First Contact or Durham Police

h. Online Radicalisation and Extremism

• We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
• If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.
• If we are concerned that member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

11. Useful Links for Educational Settings

• Education Durham

  Paul Hodgkinson, EDA with responsibility for Online Safety. 03000265841 (paul.hodgkinson@durham.gov.uk)

  Guidance for Educational Settings:
  • Extranet ( Pupils -> safeguarding -> Online Safety )
  • Kent Online Safety Blog:
    www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

• Durham LSCB:
  http://www.durham-lscb.org.uk/

• Durham Police:
  In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact the Police via 101 Prevent Officer – Steven Holden but referrals should be made through First Contact

• Other:
  • ICTSS helpdesk 03000 265841
  • Sharon Lewis (LADO) 03000 268838

National Links and Resources for Educational Settings

• CEOP:
  o www.thinkuknow.co.uk
  o www.ceop.police.uk
• Childnet: www.childnet.com
• Internet Matters: www.internetmatters.org
● Internet Watch Foundation (IWF): www.iwf.org.uk
● Lucy Faithfull Foundation: www.lucyfaithfull.org
● NSPCC: www.nspcc.org.uk/onlinesafety
  ○ ChildLine: www.childline.org.uk
  ○ Net Aware: www.net-aware.org.uk
● The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
● UK Safer Internet Centre: www.saferinternet.org.uk
  ○ Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
● 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers
● Action Fraud: www.actionfraud.police.uk
● CEOP:
  ○ www.thinkuknow.co.uk
  ○ www.ceop.police.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
● NSPCC: www.nspcc.org.uk/onlinesafety
  ○ ChildLine: www.childline.org.uk
  ○ Net Aware: www.net-aware.org.uk
● The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
● UK Safer Internet Centre: www.saferinternet.org.uk

12. **Staff and Student ICT Usage Agreements (Appendices)**

The following documents must be agreed to, signed and returned to the college before access to and use of ICT can be given to any member of staff or student.

**Appendix 1** Responsible Internet & Computer Use (Staff Agreement)

**Appendix 2** Responsible Internet & Computer Use (Student Agreement)

**Appendix 3** Parent’s Consent for Internet Access

**Appendix 4** Laptop / Tablet Usage Agreement (Staff)

**Appendix 5** Tablet device Responsible Usage Agreement (Student)
Appendix 1

Sedgefield Community College Responsible Internet & Computer Use (Staff Agreement)

The computer system is owned by the College. This Responsible Use statement helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

Staff requesting Internet access should agree to and sign a copy of this Acceptable Use Statement and return it to Gillian Bell.

- Network access must be made via the user’s authorised account username and password, which must not be given to any other person.
- All users of Sedgefield Community College systems are given a Username and Password; these are unique and must be kept secret. You must not share your password with anyone and you will be held responsible for all activity using your credentials. All passwords must conform to the following specification:
  
  1. At least 8 characters long;
  2. Require alpha and numeric elements;
  3. You are prevented from reusing the last 5 passwords;
  4. There must be a maximum of sixty days between password changes.

- School computer and Internet use must be appropriate to the student’s education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers. Users are responsible for e-mail they send and for contacts made.

The following behaviour by an employee is considered unacceptable:

I. use of college communications systems for personal use
II. forwarding of company confidential messages to external locations
III. distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
IV. distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
V. breaking into the college’s or another organisation’s system or unauthorised use of a password/mailbox
VI. broadcasting unsolicited personal views on social, political, religious or other non-college related matters
VII. transmitting unsolicited commercial or advertising material
VIII. undertaking deliberate activities that waste staff effort or networked resources
IX. introducing any form of computer virus or malware into the corporate network

- Anonymous messages and chain letters are not permitted.
- The use of chat rooms and social networking sites is not allowed. (Staff should refer to the college ‘The use of social networking applications Policy’ and associated guidance for employees).
- Staff must never present digital media to students without first checking that the content is appropriate.
• ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.

• All external storage devices must be encrypted by the MSU. This includes external hard drives and USB keys. These should be used for school work only.

• Staff must promptly report all faults or damage to ICT equipment via the ICT helpdesk. Only ICT technical support staff should carry out repairs (appropriate to their skill level).

• I understand that the school may check my computer files and the Internet sites I visit.

The school may exercise its right to monitor the use of the school’s computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school’s computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Sanctions

Where it is believed that an employee has failed to comply with this policy, they will face college disciplinary action including dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record.

Staff Agreement

I have read and I understand the school Rules for Responsible Internet & Computer Use. I understand that a breach of the conditions of ICT use outlined in this document may result in disciplinary action including dismissal.

Signed: ___________________________ Date: ___________________________

Please print name: ___________________________
Appendix 2

Sedgefield Community College Responsible Internet & Computer Use (Student Agreement)

The computer system is owned by the College. This Responsible Use statement helps to protect students, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

Students requesting Internet access should agree to and sign a copy of this Acceptable Use Statement and return it to Mr de Leeuw-Kent (Director of ICT systems) for approval and internet activation.

- Irresponsible use may result in the loss of Internet access.
- Network access must be made via the user’s authorised account username and password, which must not be given to any other person. All users of Sedgefield Community College systems are given a Username and Password; these are unique and must be kept secret. You must not share your password with anyone and you will be held responsible for all activity using your credentials. All passwords must conform to the following specification:

  5. At least 8 characters long;
  6. Require alpha and numeric elements;
  7. You are prevented from reusing the last 5 passwords;
  8. There must be a maximum of sixty days between password changes.

- School computer and Internet use must be appropriate to the student’s education or to staff professional activity.
- Copyright and intellectual property rights must be respected.
- E-mail should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers. Users are responsible for e-mail they send and for contacts made. The following behaviour by a student is considered unacceptable:

  X. use of college communications systems to set up and send chain letters
  XI. forwarding of college confidential messages to external locations
  XII. distributing, disseminating or storing images, text or materials that might be considered indecent or illegal
  XIII. distributing, disseminating or storing images, text or materials that might be considered offensive, abusive or promoting extremist views.
  XIV. accessing copyrighted information in a way that violates the copyright
  XV. breaking into the college’s or another organisation’s system or unauthorised use of a password/mailbox
  XVI. undertaking deliberate activities that waste staff effort or networked resources
  XVII. introducing any form of computer virus or malware into the corporate network

- Anonymous messages and chain letters are not permitted.
- The use of chat rooms and social networking sites is not allowed.
- ICT system security must be respected; it is a criminal offence to use a computer for a purpose not permitted by the system owner.
- USB keys should be used for school work only.
- Respect all hardware. Don’t touch the back of machines.
- Do not bring food or drink into ICT areas, including chewing gum.
- I understand that the school may check my computer files and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right to monitor the use of the school’s computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school’s computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

**Pupil’s Agreement**

I have read and I understand the school Rules for Responsible Internet & Computer Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.

Signed: ___________________________  Date: ___________________________

Please print name: ___________________________

Tutor Group: _______________  User name: _______________

**E-Safety and Online ICT Policy**

Sedgefield Community College
Appendix 3

Parent’s Consent for Internet Access

I have read and understood the school Rules for Responsible Internet & Computer use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: ________________________________________ Date: _______________________

Please print name: _____________________________________________________________

ICT Staff signature: ____________________________ Date: _________________________
Appendix 4

Laptop/Tablet Usage Agreement (Staff)

What is the Policy- The policy outlines the responsibilities that Sedgefield Community College staff must accept when they are issued a laptop.

Who is affected by the policy- This policy applies to members of staff within Sedgefield Community College who have been issued with a laptop/tablet.

Why was this policy created- Laptops/tablets provide the convenience of portability. This convenience exposes the college to certain risks. These include but are not limited to:

- Theft of college property
- Laptops/tablets are easy to steal and their relatively high value and easiness to sell makes them common targets of theft
- Exposure of sensitive data or information
- Misplaced or unsecured laptops/tablets may expose sensitive information to the public. Loss of such data could be utilised by sections of the public for illegal purposes
- Damage of college property
- Laptops/tablets can be susceptible to damage both due to their nature and their relatively fragile construction.

What do I need to do- Any member of staff issued with a laptop/tablet will need to confirm, by signing the acceptance on this policy, that he/she has read, understands and will comply with the policy. The policy will need to be signed by the member of staff, with a copy kept within the Personnel department until the laptop is returned or replaced.

Sedgefield Community College Laptop/Tablet Usage Policy – The laptop/tablet is the property of Sedgefield Community College and is to be returned to the ICT staff before your contract end date. In the event of any long term absence the laptop/tablet will need to be returned. When a Sedgefield Community College staff member is provided with a laptop/tablet, he/she accepts responsibility for safeguarding the laptop/tablet itself as well as the data stored on the laptop/tablet. Laptop/tablet Users are expected to exercise reasonable care and take the following precautions;

- Ensure they have appropriate car and house insurance to be able to transport/ use the laptop/tablet out of school.
- Take appropriate steps to protect the laptop/tablet from theft:
  - Laptops/tablets should not be left in an unattended office without closing and locking the door
  - Laptops/tablets should not be left out overnight in offices, and should always be locked away
  - Laptops/tablets, where possible, should not be left unattended in a parked car. On those occasions where there is no alternative, they should be locked in the boot.
  - Laptops/tablets should be carried and stored in a padded laptop/tablet bag/case or strong briefcase to reduce the chance of accidental damage
- Keep a note of the Laptop/tablet’s serial number. If the laptop/tablet is lost or stolen the IT Service Desk will need this number to assist with insurance requirements.
- Do not work or save sensitive information on a laptop/tablet without taking appropriate precautions;
Sensitive information refers to any data that is protected by the authority policy, or by any local, or national laws or regulations. This includes but is not limited to; education records, personally identifiable information and confidential internal Authority information.

All members of staff are accountable for all networks and systems access under their user ID, so passwords should be kept absolutely secret. It should never be shared with anyone.

Corporate laptops/tablets are provided for official use by authorised employees.

College laptops/tablets must not be loaned or be allowed to be used by others.

Avoid leaving your laptop/tablet unattended and logged on. Always shut down, log off or lock the screen before walking away from the machine.

**Take care to protect the laptop/tablet from damage**

- Laptops/tablets should not be used in environments that might increase the likelihood of damage
- Laptops/tablets should be kept in a padded carrying case or sleeve during transportation

**Virus Protection**

- Viruses are a major threat to the college and laptops are particularly vulnerable if their anti-virus software is not kept up to date. The antivirus software must be updated at least monthly. The easiest way of doing this is simply to log onto the school network for the automatic update process to run
- Email attachments are one of the main sources of computer viruses. Avoid opening any email attachments unless they are expected from a legitimate source
- Report any security incidents (such as virus infections) promptly to the ICT staff in order to minimize the risk of damage

**Software Installations**

- Do not download, install or use unauthorized software programs. Any software that is required to be installed must be installed through the ICT Service. The ICT service will need to have proof of license and will store the license securely for audit purposes

**Laws, regulations and policies**

- You must comply with relevant laws, regulations and policies applying to the use of computers and information. Software licensing has already been mentioned and privacy laws are another example

**Inappropriate materials**

- Sedgefield Community College will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or email messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop/tablet and steer clear of dubious websites

**Health and Safety aspects of using laptops**

- Laptops/tablets normally have smaller keyboards, displays and pointing devices that are less comfortable to use than desktop systems, increasing the chance of repetitive strain injury. Where possible, place the laptop/tablet on a conventional desk or table
- If you tend to use the laptop/tablet in an office most of the time, request a normal keyboard, mouse and screen from the ICT staff. If you experience symptoms such as wrist pain, eye strain or headaches that you think may be caused or exacerbated by your use of the laptop/tablet, stop using the laptop and consult with Occupational Health at the earliest convenient time

**Report Damage or Loss as soon as possible**

Any damage or loss must be reported to the relevant line manager, Mr Robinson (Deputy Headteacher) and the IT support team. Failure to comply with this policy could lead to disciplinary action.

If you have questions about the policy, please contact the ICT staff on 01740 617777.

**Staff Agreement**

I have read and I understand the laptop/tablet usage policy. I will use the laptop/tablet in a responsible way and obey these rules at all times.
Signed: ___________________________  Date: ___________________________

Please print name: ______________________

Serial Number: ______________________

Asset Tag No. : ______________________
Appendix 5

Tablet device Responsible Usage Agreement (Student)

Enhancing Learning through Technology

At Sedgefield Community College we believe that using technology in school and at home brings learning into the 21st century. It gives learners the opportunity to learn at their own pace, and for learning at home to be more structured and effective.

We believe that tablet technology will give every learner the opportunity to progress faster and achieve more. We also believe that it will help to strengthen relationships between home and school. For this reason we aim to support parents to provide their child with a student device to be used throughout years 9, 10 and 11.

We are determined to ensure that the tablet devices are only used in lessons when there are clear educational advantages to doing so. We want the tablet device to become a useful tool for learning and for setting far more challenging and engaging home learning experiences.

We are aware of the risks associated with using new technology in this way and we have tried to provide guidelines on how we work to manage these risks as much as possible.

Yours Sincerely,

Craig Hutton
Assistant Head teacher
Sedgefield Community College
HOME SCHOOL AGREEMENT

To help ensure that our 1:1 programme is a big success at Sedgefield Community College and that we get maximum value from our joint investment in your children, we invite you to commit to the principles outlined in this agreement. As a school we are prepared to provide all of the back-up and resources needed to make this work, but we also need the commitment of parents and students.

As you read through this leaflet you will see a summary of our 1:1 programme commitment that the school is making to the students and to you as parents. It also outlines the commitment that will be needed from the home, and from the children themselves, to make this work.

When you have read these sections we invite you and your child to sign the agreement and return it to school. This will help to ensure that we are all working together to achieve success.

Remember that using a Samsung Galaxy Tab (referred to as the ‘device’ in this leaflet) is a privilege, not a right, and should be used in a responsible and ethical manner at all times.

TERMS & CONDITIONS

- Failure to take reasonable care or to abide by the other conditions in this document may result in the device being reclaimed. The school reserves the right to claim financial recompense in such cases
- The device should be charged at home overnight, but the school cannot accept responsibility for electricity costs
- Ensure that the device is returned either at the end of the programme or if the student leaves the school for whatever reason before then, or at any other time upon the request of a member of staff. Unless the parent has made the full contribution needed, in which case the parent may keep the device.

THEFT:

A stolen device must be reported to the police as soon as possible and a crime number assigned. From there the parent should contact the insurance company directly. Details of how to do this are available on the schools website. Please note, the insurance company may not settle the claim in the following circumstances;

- The device was left in plain view in an open bag or unlocked locker, car or house
- The device was stolen due to negligence, careless behaviour or unwise use in or out of school

SOFTWARE:

The device has all of the necessary software pre-installed onto it in regards to the operating system and basic features and functionality. Predominately the device is used to access the schools Learning Platform but there may be occasions additional ‘apps’ may need to be purchased from the ‘App store’ on the device. Where possible, the apps will either be free of charge or purchased by the school.

Apps by their nature are very cheap and we envisage any parental purchases to be minimal and often a cheaper replacement for something else, for example the purchase of an ‘e-book’ rather than a text book.

THE SCHOOL WILL:

- Provide a device for your child’s use, for the length of the programme
• Provide a case to protect the device
• Provide the Apps and Resources required for educational purposes (aside from what is described above)
• Make sure that the device is covered by insurance for use in and out of school for study purposes, providing reasonable care is taken to prevent loss (through theft) or damage
• Provide secure storage for the device when it is not needed for any particular lesson
• Provide on-going support for the device
• Ensure that the device is protected against computer viruses
• Teach students to use the device safely
• Monitor the use of the device both remotely and directly in and around school

AT HOME WE WILL:

• Ensure that our child understands how to care for and protect their device
• Report any loss or damage (including accidental loss or damage) within one week
• Report any faults in hardware or software promptly
• Ensure that your child understands that the device is primarily for educational purposes and that it is always in a state to work with
• Pay a contribution toward the cost of a second and third breakage (see ‘Broken Device’ section for details)
• Ensure that the device is fully charged ready for school use each day.

Our expectations of student’s use of their tablet devices

THE STUDENTS WILL BE EXPECTED TO:

• Look after the device very carefully all of the time. It will be kept in its case at all times and stored securely when not in the students possession
• Take responsibility for setting up a secure password and not sharing it with other students
• Create a lock screen for the device which shows name and tutor group
• Bring it to school every day fully charged, unless told not to
• Take care when the device is transported so that it is as secure as possible (e.g. not visible in a vehicle / not left unattended on a bus / etc.)
• Make sure the device is not subject to careless or malicious damage (e.g. as a result of horseplay)
• Ensure the device is only used for educational purposes whilst in school
• Regularly back up the device as instructed by the school
• Allow staff to access the device to check for inappropriate materials. Understand that staff will be allowed to remove inappropriate resources
• Always act on the advice of the school in the safe use of this device
A STUDENT WILL NOT:

- Use the device for any form of cyber bullying or for sending, accessing, uploading or distributing any insulting, threatening, pornographic, violent or obscene material
- Use the device for sending mass emails (spamming)
- Remove the device from its case
- Use the school email account for any form of commercial or financial gain
- Take photographs or videos without the permission of the subject teacher, or upload or share these images with anyone without the permission of the subject teacher.
- Install age-inappropriate games and content
- Use any software or other method to break any of the security systems in place on the device. Any detection of this kind of software will result in sanctions and possible temporary confiscation
- Use the device to access VPN (virtual private networks). These apps whilst available on the App store allow the user to bypass any school internet security protocols and access blocked websites or social networking sites
- Physically decorate, customise or use graffiti on the device or its case
- Delete any pre-installed software, in particular try to remove the Mobile Device Management software that the school uses to manage the device when in-school.
- Use the device for any illegal and/or anti-social purpose, including access to inappropriate websites

BROKEN DEVICE:
Unfortunately, devices on occasion do get broken and this is the procedure should the need arise.

A broken device must be reported straight away as we only have a week’s window to claim on the insurance, even if it is during the holidays. All breakages must be reported even if it is a tiny crack in the screen and a form must be completed. The insurance companies do have forms online and it will therefore be the parent’s responsibility to report the damage (this is simply due to damage potentially occurring during the school holidays). The insurance company will also collect, fix and return the device to any UK address. All information and links to the relevant forms are available on the school website.

1st & 2nd Breakage: your device will be returned to you and the insurance will cover the repair
3rd Breakage: you will be responsible for a £10 charge that will go towards the repair of the device. Payment should be completed through the school and the device will not be sent off for repair until payment has been received.
4th Breakage: you will be asked to contribute a further £25 and also choose between one of the two following options:
   1. You can opt out of the scheme and the device can only be used in school. It can be collected first thing in the morning and must be returned after final lesson of the day
   2. You can remain in the scheme but must commit to contributing £25 for each future claim for repair of the device following any future damage

Note; the contributions to the repair may come from the deposit the school is holding.

We will not support the following breakages and therefore you will be required to pay for them:
- Deliberate and wilful damage to the device
- Any problems resulting from device that has been ‘Jailbroken’
- Where the damage was damaged as a result of not being in its protective case
During the time it takes to repair the device we have a limited stock of loan devices for use during the school day which must be returned after the last lesson.

**Appropriate use in School**

**In lessons**
Some teachers will use the tablet devices in lessons more than others. Your use of the tablet device in school is always at the teacher’s discretion. If the teacher hasn’t asked you to use the tablet then it should be kept out the way in your school bag. If the teacher feels that you have not been using the device responsibly then they will ask you to put it away and will issue a suitable consequence in-line with our Behaviour for Learning Policy.

**Break/Lunchtimes**
We do want to encourage students to work collaboratively with their tablet devices in their own time however we feel strongly that it is essential that students spend time away from the device and take a break.
The tablet should not be used outside, or inside the school building at break or lunchtime and should be stored securely in your locker or bag. The only time it is acceptable is in a designated room in your year area.

**General**
Students should be aware that staff may review files and communications to ensure that users are using the system responsibly; users should not expect that stored files would always be private.

During school, teachers will guide students toward appropriate materials. Outside of school, families bear responsibility for such guidance as they must do currently with information sources such as television, telephones, movies, radio and other potentially offensive media.

The following are not permitted:
1. Sending or displaying offensive messages or pictures
2. Using obscene language
3. Harassing, insulting or attacking others
4. Damaging computers, tablet devices, computer systems or computer networks
5. Violating copyright laws
6. Using others’ passwords
7. Trespassing in others’ folders, work or files
8. Intentionally wasting limited resources
9. Removing the MDM profile

**Consequences**
1. Violations of the above rules will result in a temporary or permanent ban on Internet use or use of school ICT equipment in general.
2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
3. When applicable, police or local authorities may be involved.
Using the Camera
Issues about photographing staff and students are already covered in other policies, however it is important to be aware that some staff and students are not prepared to have their photograph taken and that permission must always be sought first.

Email Etiquette
Email is likely to become a key means of communication between staff and students. It is important that students are aware of the rules regarding this area and do not cause offence or add needlessly to staff workload.
Wherever possible avoid using emails to staff. If you are able to go and find that member of staff personally and speak to them directly then this is always preferable.
Any essential emails to staff, such as those sent to hand in work, should always be politely written. Start the email with Sir/Miss or the member of staff’s name and always end with ‘Thank you’ and your name.

Health & Well-Being:

Personal Safety
The likelihood of being approached outside of school by someone trying to steal the tablet device is slim, but it is important that all students act safely to limit this risk.
Ensure that the device is kept in your bag when walking to and from school. Follow the usual advice about keeping safe, for example not walking around alone when it is dark and ensuring that an adult knows where you are. If approached, just hand the tablet device over and report the incident to the police to obtain a crime number before proceeding with an insurance claim.

eSafety
Many of the eSafety issues that apply to the use of tablet devices already exist within school and have been addressed in our eSafety Policy. When accessing the internet on the device, you are agreeing to follow the rules outlined in the schools ‘Acceptable Usage Agreement’ as you currently do when accessing the internet in-school on any school computer.
Please be aware that a member of staff has the right to look at the content stored on your tablet device at any time and this will happen as part of random spot checks to ensure that the tablet devices are being used appropriately.
Please complete and sign this form and return it to the school as soon as possible:

**STUDENT’S AGREEMENT**
I agree to abide by these terms in my use of the Samsung Galaxy Tab

Name: ___________________________________________________________ Tutor Group: ______

Signed: __________________________________________________________ Date: __________________

**PARENT’S AGREEMENT**
I agree to my child having the use of the Samsung Galaxy Tab on these terms

Signed: __________________________________________________________ Date: __________________

**HEADTEACHER’S AGREEMENT**
I agree on behalf of the school to provide a Samsung Galaxy Tab on these terms

Signed: __________________________________________________________ Date: __________________