Education
Partnership
NorthEast

Hartlepool SixthForm | Sunderland College | Northumberland College

E safety Policy

Review

Formal Review Cycle	Annually		
Latest Formal Review (date)	April 2021	Next Formal Review Due (date)	April 2022
Policy Owner	Nicola Warburton		
Policy Author	Nicola Warburton		

Approvals

Board of Corp Y/N		Committee		Date Board approved	
SLT Y/N	Y	SLT date approved		Additional committee	

Publication

Website Y/N	Y	Intranet Y/N	Y	Student VLE Y/N	Y	Other	

Change History

Version	Date Reviewed/ Revised	Description of Change	Reviewed by	Approved by

E-safety Policy

1. Policy Statement

1.1. This policy is a policy of the City of Sunderland College, trading as Education Partnership North East (which includes Sunderland College, Hartlepool Sixth Form College and Northumberland College). These colleges will be referred to as “the College” throughout this document.

1.2. EPNE withholds the right to instigate disciplinary procedures for inappropriate use / behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of college, but are linked to EPNE.

1.3. EPNE will deal with such incidents within this policy and associated use / behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of college.

2. Scope

2.1 This Policy applies to all those working in, studying and visiting any College site including students, the College workforce, Governors, volunteers and visitors to the College including contracted services such as agency staff, employers offering work placements, transportation companies, sub-contractors and contractors with direct access to children, young people and vulnerable adults.

2.2. Students aged 14-16 whose main education provider is a School are covered by all aspects of the Policy when at the College. In accordance with agreed partnership protocols, there is a separate procedure for Child Protection referrals as schools retain accountability for external referrals. Should there be an emergency and the College is unable to contact the appropriate school, the College will apply its referral procedures to the situation to ensure a child is safe.

2.3. Employers and sub-contractors will be asked to make a commitment to safeguarding students’ welfare by endorsing an agreed statement of principles. Any person whose normal duties include regular caring for, training, looking after or supervising a child in the workplace where that person has been specifically designated to have responsibility for such activities will be subjected to vetting and DBS checking. Providers will be monitored annually for compliance with process and must report any incidents to the college for any subcontracted provision. For employers providing apprenticeship and/or industry placements, DBS checking will be undertaken on a risk-based approach.

2.4. For apprenticeships and long-term placements, the College will ensure that additional safeguards are in place, these must include staff who will have had training in child protection, completing risk assessments and arranging placements.

3. Aims of the Policy/Underpinning Principles

3.1. E-Safety is about safe and responsible practice with technology and the sensible management of risks presented by the digital world. There is a need to educate ourselves and others about the benefits and risks of using technology and to provide awareness, skills and safeguards to enable users to take responsibility for their own and others’ online experience. The aim of this policy is to:

3.1.1. Educate students to allow them to safely live in a digital society.

3.1.2. Providing a clear framework for managing online safety.

3.1.3. Educate staff and students to take responsibility and be able to safeguard themselves and their personal information.

3.2. The College values diversity and inclusion and is committed to promoting equal opportunities and eliminating discrimination. Therefore, staff will apply and administer this policy fairly and consistently to ensure that there is no discrimination on the grounds of age, disability, gender reassignment, marital and civil partnership status, pregnancy and maternity, race, religion or belief, sex, sexual orientation, (and for student facing policies include) young persons in care and care leavers, young carers and care givers, young parents, youth offenders, and those receiving free school meals.

4. Responsibilities

Senior Leadership and Governors is responsible for ensuring that:

- Have a duty of care for ensuring the safety (including e-safety) of members of the college community, although the day to day responsibility for e-safety will be delegated to the Head of Student Services.
- Designate a member of the senior management team, should there be a serious e-safety allegation being made against a member of staff.
- Ensure that there is a system in place to allow for monitoring and support of those who carry out the internal e-safety monitoring role.
- Responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by receiving regular information about e-safety incidents and monitoring reports.

Director of Student Services is responsible for ensuring that:

- Lead e-safety
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Receive reports of e-safety incidents and creates a log of incidents to inform future esafety developments
- Meet regularly and Director of IT Services to discuss current issues and review incident logs
- Report regularly to the Senior Management Team
- Embed safety into Induction for all students

Head of Student Services is responsible for ensuring that:

- Take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the e-safety policy
- Provide training and advice for staff
- Liaise with technical staff
- Liaise with the Local Authority / relevant body

Intensive Support Manager is responsible for ensuring that:

- Meet regularly with Head of Student Services to discuss current issues and review incident logs
- Attend relevant meetings
- Where safeguarding concerns exist, co-ordinate with external agencies
- Check firewall daily and identify students who need intervention

People and Development are responsible for**:**

- Monitoring the staff Firewall

Director or ICT is responsible for ensuring that:

- The colleges technical infrastructure is secure and is not open to misuse or malicious attack

- The college meets required e-safety technical requirements
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- They keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- The use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of Student Services for investigation / action / sanction
- Monitoring software / systems are implemented and updated

Designated Safeguarding Lead is responsible for ensuring that:

- They share with the Head of Student Services, issues or concerns disclosed during safeguarding meetings with students.

Teaching, Safeguarding and Support Staff Teaching is responsible for ensuring that:

- They have an up to date awareness of e-safety matters
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Head of Student Services
- All digital communications with students / parents / carers should be on a professional level and only carried out using official EPNE systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the e-safety and acceptable use policies EPNE - E-Safety Policy & Procedures
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other activities and implement current policies with regard to these devices.
- In lessons, where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Parents/Carers is responsible for ensuring that:
Parents / Carers play a crucial role in ensuring that their child understands the need to use the internet / mobile devices in an appropriate way. The college will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the college in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at college events
- Parents' sections of the website / VLE and on-line student records
- Their child's personal devices in the college.

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the student's on-line behaviours. Parents may underestimate how often students come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. EPNE will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, etc.…
- Parents / Carers evenings / sessions
- High profile events / campaigns

Partners/Employers are responsible for ensuring that:
Users who access EPNE systems will be expected to sign an Acceptable Use Agreement before being provided with access to EPNE systems.

Students is responsible for ensuring that:
Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of EPNE's e-safety provision. Students need the help and support of the college to recognise and avoid e-safety risks and build their resilience.
E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Key e-safety messages should be reinforced as part of a planned programme tutorial and other pastoral activities
- Students should be taught in lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet EPNE - E-Safety Policy & Procedures
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside EPNE. This includes accepting monies paid for posting inappropriate content on social media sites.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where students can freely search the internet, staff should be vigilant in monitoring the content of the websites they visit
- It is accepted that, from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs or discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that IT Services temporarily remove those sites from the filtered list for the period of study. Any request to do so should be placed with the IT Helpdesk, with clear reasons for the need

5. Implementation

(Policy process or procedures, defined terms, compliance and potential repercussions for violating the policy.)

5.1. Education and Training

5.1.1. It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly EPNE - E-Safety Policy & Procedures
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the college e-safety policy and Acceptable Use Agreements
- The Head of Student Services will receive regular updates through attendance at external training events
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings

- The Head of Student Services will provide advice / guidance / training to individuals as required

5.2. Technical – infrastructure / equipment, filtering and monitoring

5.2.1 It is the responsibility of the Director of IT Services to carry out all the e-safety measures.

5.2.2 The Director of IT Services will be responsible for ensuring that the college IT infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

Technical systems will be managed in ways that ensure that EPNE meets recommended technical requirements. There will be regular reviews and audits of the safety and security of the college technical systems.

Servers, wireless systems and cabling must be securely located and physical access restricted

All users will have clearly defined access rights to technical systems and devices. All users will be provided with a username and secure password. The Director of IT Services will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be requested to change their password every six months

The "master / administrator" passwords for the IT infrastructure must also be made available to the Principal

- The Director of IT Services is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations
- Internet access is filtered for all users and content lists are regularly updated and internet use is logged and regularly monitored
- EPNE technical staff regularly monitor and record the activity of users on the college IT systems and users are made aware of this in the Acceptable Use Agreement EPNE - E-Safety Policy & Procedures
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the IT Help Desk
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of college systems and data. These are tested regularly. The college infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests"
- An agreed policy is in place that allows staff to download executable files and installing programmes on college devices
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on EPNE devices. Personal data cannot be sent over the internet or taken off site unless safely encrypted or otherwise secured.

5.3. Student Devices

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by colleges of users bringing in their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations that need to be reviewed prior to implementing such a policy. Use of students' own devices should not introduce vulnerabilities into existing secure environments. Considerations will need to include: levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive

- EPNE has a set of clear expectations and responsibilities for all users

- EPNE adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the college's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance EPNE - E-Safety Policy & Procedures
- Students and staff must be made aware that their usage while on college premises is monitored to ensure compliance.

5.4. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. EPNE will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Staff can take digital / video images to support educational aims, but must follow college policies concerning the sharing, distribution and publication of those images
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the college into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of students are published on the college website
- Students' work can only be published with the permission of the student and parents or carers.

5.5. Data Protection and GDPR

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights

- Secure
- Only transferred to others with adequate protection.
- EPNE will ensure that:
  It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for

  *Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
  *All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing"
  *It has a Data Protection Policy
  *It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
  *Risk assessments are carried out
  *It has clear and understood arrangements for the security, storage and transfer of personal data
  *Data subjects have rights of access and there are clear procedures for this to be obtained
  *There are clear and understood policies and routines for the deletion and disposal of data
  *There is a policy for reporting, logging, managing and recovering from information risk incidents

  - There are clear Data Protection clauses in all contracts where personal data may be passed to third parties EPNE - E-Safety Policy & Procedures
  - There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.
- **Staff must ensure that they:**
  At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. They must use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data. Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, memory stick or any other removable media:
- The data must be encrypted and password protected
- The device must be password protected (memory sticks / cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with college policy, once it has been transferred or its use is complete
- Staff must adhere to the ICT policy when accessing college network remotely

5.6. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. Refer to the EPNE Acceptable Use of Social Media policy for further advice. General principles are outlined below.

When using communication technologies EPNE considers the following as good practice:

- The college email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the college email service to communicate with others

- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication EPNE - E-Safety Policy & Procedures
- Any digital communication between staff and students must be professional in tone and content. These communications may only take place on official systems. Personal email addresses, text messaging or social media must not be used for these communications
- Staff should not give out their personal home or mobile telephone number to students. The college provides mobile phones for educational visits and this number should be given to students / parents.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the college website and only official email addresses should be used to identify members of staff.

5.7. Social Media - Protecting Professional Identity

5.7.1 Please refer to The Acceptable Use of Social Media Policy. General principles are outlined below.

5.7.2 EPNE provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the college through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

5.7.3 Staff should ensure that:

- No reference should be made in social media to students or staff
- They do not engage in online discussion on personal matters relating to members of the college community
- Personal opinions should not be attributed to EPNE

5.8. Unsuitable / Inappropriate Activities

5.8.1 EPNE considers that the activities referred to in the following section would be inappropriate in a college context and that users, as defined below, should not engage in these activities on site or outside college using college property / networks. The college policy restricts usage as follows:

5.8.2 Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images
- Grooming, incitement, arrangement or facilitation of sexual acts
- Youth produced sexual imagery (formally known as sexting)
- Criminally racist material in UK – to stir up religious hatred
- Pornography
- Promotion of any kind of discrimination
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of EPNE’s or brings the college into disrepute
- Using college systems to run a private business

- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the college
- Infringing copyright
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet)
- On-line gaming other than for educational purposes
- On-line gambling
- On-line shopping / commerce
- File sharing
- Use of social media
- Use of messaging apps
- Use of video broadcasting
- Students and staff must be made aware that their usage while on college premises is monitored to ensure compliance.

5.9 Responding to incidents of misuse

5.9.1 This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

5.9.2 Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to Intensive Support Manager or Head of Student Services.

5.9.3 Other Incidents

It is hoped that all members of the college community will be responsible users of digital technologies. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

5.9.4 Intensive Support Manager will monitor the College Firewall on a daily basis for students. People and Development will monitor this for staff.

5.10 College Actions and Sanctions

5.10.1 Students

The following points represent general principles in deciding if any actions or sanctions will be taken. In all cases, refer to the student positive behaviour policy in the first instance.

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)
- Unauthorised use of non-educational sites during lessons
- Unauthorised use of mobile phone / digital camera / other mobile device
- Unauthorised use of social media / messaging apps / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access the college network by sharing username and passwords
- Attempting to access or accessing the college network, using another student’s account
- Attempting to access or accessing the college network, using the account of a member of staff
- Corrupting or destroying the data of other users

- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring the college into disrepute or breach the integrity of the ethos of EPNE
- Using proxy sites or other means to subvert the college's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.

5.10.2 Staff

The following points represent general principles in deciding if any actions or sanctions will be taken. In all cases, refer to the staff disciplinary policy in the first instance.

- Deliberately accessing or trying to access material that could be considered inappropriate
- Inappropriate personal use of the internet / social media / personal email EPNE - E-Safety Policy & Procedures
- Unauthorised downloading or uploading of files
- Allowing others to access college network by sharing username and passwords or attempting to access or accessing the college network, using another person's account
- Careless use of personal data e.g. holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students
- Actions which could compromise the staff member's professional standing
- Actions which could bring the college into disrepute or breach the integrity of the ethos of the college
- Using proxy sites or other means to subvert the college's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Breaching copyright or licensing regulations
- Continued infringements of the above, following previous warnings or sanctions

6. Associated Documents

(Related pertinent policies, procedures, guidelines, legislation, regulations, collective agreements, etc. and documents that provide supplemental information to the policy.)

7. Policy Monitoring and Review

(How is policy effectiveness going to be monitored? How often is the policy to be reviewed?)

7.1 The implementation of this E-Safety Policy will be monitored by the following:

- Designated Safeguarding Lead
- Director of Student Services
- Head of Student Services

- Personal Development and Wellbeing Leads
- Director of IT

7.2 The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

8. Equality Impact Assessment

(Consider whether the policy or procedures may disproportionately impact any group.)

Have you sought consultation on this policy? **Details:**		Yes Intensive Support Manager Director of Student Services Intensive Support Officers		
Could a particular group be affected (negatively or positively)?	**Impact Y/N**	**Description of Impact**	**Evidence**	**Mitigation/ Justification**
Protected characteristics under the Equality Act 2010				
Age	N			
Disability	N			
Gender Reassignment	N			
Marriage and Civil Partnership	N			
Pregnancy and maternity	N			
Race	N			
Religion or belief	N			
Sex	N			
Sexual Orientation	N			
Additional characteristics to consider				
Young Persons in Care & Care Leavers	Y	Designated staff members in place		
Young Carers & Care Givers	Y	Designated staff members in place		
Young Parents	Y	Designated staff members in place		
Youth Offenders	Y	Designated staff members in place		
Those Receiving Free School Meals	Y	Designated staff members in place		
If there is no impact, please explain:				