



E-Safety Policy

1. Policy Aims

This online safety policy takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2018 and the Northamptonshire Safeguarding Children Board procedures.

In this policy, the term 'the Youth Works Northamptonshire community' refers to all staff, volunteers, trustees, students, service users, parents, carers and external contractors.

The terms Chief Executive Officer (CEO) and Head Teacher are used interchangeably and refer to the same person.

- The purpose of Youth Works Northamptonshire's online safety policy is to:
 - Safeguard and protect all members of the Youth Works 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.
- Youth Works Northamptonshire 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

- Youth Works Northamptonshire believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harm online.
- Youth Works Northamptonshire identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

- Youth Works Northamptonshire believes that young people should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff (including manager, tutors, support staff, volunteers, the Board of Trustees, external contractors and other individuals who work for, or provide services on behalf of the organisation collectively referred to as 'staff' in this policy) as well as young people and parents/carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where young people, staff or other individuals have been provided with organisation issued devices for use off-site, such as a work laptops, tablets or mobile phones.

Links with other policies and practices

- This policy links with a number of other policies, practices and action plans including:
 - Anti-bullying policy
 - Acceptable Use Policies (AUP)
 - Behaviour policy
 - Confidentiality policy
 - Data protection policy
 - Disciplinary policy
 - Safeguarding policy

3. Monitoring and Review

- Youth Works Northamptonshire's Board of Trustees 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 ensure that we 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 CEO will be informed of online safety concerns, as appropriate.
- The named Trustee for safeguarding will report on a regular basis to the Board on online safety incidents, including outcomes.
- Any issues identified will be incorporated into the organisation's action planning.

4. Roles and Responsibilities

- The Organisation has appointed Carole Carson, as Designated Safeguarding Lead to be the online safety lead.
- Youth Works Northamptonshire recognises that all members of the organisation have important roles and responsibilities to play with regards to online safety.

4.1 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 an AUP.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Monitor the safety and security of the organisation's systems and networks.
- Ensure that online safety is embedded within the Youth Works Community College curriculum, enabling students to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for concerns relating to online safety with access/links to internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.

4.2 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.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the college community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- 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 organisation's 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 management team and the Board of Trustees.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet termly with the Trustee with the lead responsibility for safeguarding.

4.3 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 AUPs.
- Take responsibility for the security of the organisation's 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 Youth Works Community College curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the young people accessing our services.
- Identify online safety concerns and take appropriate action by following the organisation's 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.

4.4 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 (*including password policies and encryption*) to ensure that the college's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the organisation's filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the organisation's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the organisation's safeguarding procedures.

4.5 It is the responsibility of Youth Works Community College students and other service users (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the organisation's AUP.
- 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.

4.6 It is the responsibility of parents and carers to:

- Read the college AUP and encourage their children to adhere to them.
- Support the organisation in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from Youth Works Northamptonshire, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with students

- Youth Works Community College will establish and embed online safety in the curriculum to raise awareness and promote safe and responsible internet use amongst students by:
 - Ensuring education regarding safe and responsible use precedes internet access.
 - Including online safety in the PSHE covering use both at college and home.
 - Reinforcing online safety messages whenever technology or the internet is in use.
 - Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
 - Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The college will support students to read and understand the AUP in a way which suits their age and ability by:
 - Displaying acceptable use posters in all rooms with internet access.
 - Informing students that internet use will be monitored for safety and security purposes and in accordance with legislation.
 - Rewarding positive use of technology by students.
 - Implementing appropriate peer education approaches.
 - Providing online safety education.

- Seeking the voice of young people when writing and developing college online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support the college's internal online safety education approaches.

5.1.1 Vulnerable Students

- Youth Works Northamptonshire is aware that some students are considered to be 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.
- Youth Works Community College will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students.

5.2 Training and engagement with staff

The Organisation will:

- Provide and discuss the online safety policy 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, as part of the existing safeguarding and child protection training and updates. This will cover the potential risks posed to young people (Content, Contact and Conduct) as well as our professional practice expectations.
- Make staff aware that systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with the organisation's policies when accessing work systems and devices.
- Make staff aware that their online conduct out of work, including personal use of social media, could have an impact on their professional role and reputation within the organisation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the young people they are working with.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting young people, colleagues or other members of the Youth Works community.

5.3 Awareness and engagement with parents and carers

- Youth Works Northamptonshire recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- Youth Works Northamptonshire 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.
 - Drawing their attention to the organisation's online safety policy and expectations in newsletters, letters, our college prospectus and on our website.
 - Requesting that they read online safety information as part of joining our college.
 - Requiring them to read the organisation's AUP and discuss its implications with their children.

6. Reducing Online Risks

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

Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a Youth Works Northamptonshire computer or device.

- All members of the Youth Works Northamptonshire community are made aware of the organisation's 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 others. This is clearly outlined in the college's AUP and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

- Youth Works Community College uses a wide range of technology. This includes access to:
 - Computers, laptops and other digital devices
 - Internet which may include search engines and educational websites
 - College learning platform (Moodle)
 - Email
 - Digital cameras, web cams and video cameras
- All college owned devices will be used in accordance with the college's AUP and with appropriate safety and security measures in place such as up to date security software and the use of blocking controls where appropriate.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The college will ensure that the use of internet-derived materials, by staff and students, complies with copyright law and acknowledge the source of information.
- Students will be appropriately supervised when using technology, according to their ability and understanding

7.2 Managing Internet Access

- All staff, service users and visitors will read and sign an AUP before being given access to the organisation's computer system, IT resources or internet.

7.3 Filtering and Monitoring

7.3.1 Decision Making

- Youth Works Northamptonshire's trustees and leaders have ensured that the college has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The Trustees and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The organisation's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our organisation's 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 students; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- The organisation uses broadband connectivity through BT.
- The organisation uses BT's filtering system which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. The organisation's filtering system blocks all sites on the [Internet Watch Foundation](#) (IWF) list.

Dealing with Filtering breaches

- The organisation has a clear procedure for reporting filtering breaches.
 - If young people discover unsuitable sites, they will be required to turn off the screen and immediately report the concern to a member of staff.
 - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead.
 - The breach will be recorded and escalated as appropriate.
 - Parents/carers will be informed of filtering breaches involving their child.
- Any material that the college believes is illegal will be reported immediately to the appropriate agencies, such as: Northamptonshire Police or CEOP.

7.3.3 Monitoring

- The organisation will appropriately monitor internet use on all its owned or provided internet enabled devices. This is achieved by:
 - Physical monitoring (supervision) of use.
 - Reviewing logfile information of internet and web access.
- Any concerns identified via monitoring approaches will be reported to the Designated Safeguarding Lead who will respond in accordance with the appropriate policy e.g. behaviour policy, disciplinary policy etc.
- All users will be informed that use of the organisation's systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation. Full information can be found in Youth Works Northamptonshire's Data Protection Policy and the appropriate privacy notice. All available at www.youthworksnorthamptonshire.org.uk/about-us/Pages/policies.aspx

7.5 Security and Management of Information Systems

- The organisation takes appropriate steps to ensure the security of our information systems, including:
 - Virus protection being updated regularly.
 - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
 - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
 - Regularly checking files held on the organisation's devices.
 - The appropriate use of user logins and passwords to access the college's Learning Platform and organisation's data management systems.
 - All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password policy

All members of staff will have their own unique username and private passwords to access systems; members of staff are responsible for keeping their password private.

All college students are provided with their own unique username and private passwords to access college systems; students are responsible for keeping their password private.

We require all users to:

- Use strong passwords for access into our system which include at least one uppercase letter, lowercase letter, number and special character e.g. a punctuation mark.
- Change their passwords every 3 months.
- 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.

7.6 Managing the Safety of the Organisation Website

- The organisation will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The organisation 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 young people's personal information will not be published on our website; the contact details on the website will be the organisation address, email and telephone number.
- The administrator account for the website will be secured with an appropriately strong password.
- The organisation will post appropriate information about safeguarding, including online safety, on the website for members of the community.

7.7 Publishing Images and Videos Online

- Youth Works Northamptonshire will ensure that all images and videos shared online are used in accordance with the organisation's Data Protection Policy and Privacy Notices.

7.8 Managing Email

- Access to the organisation's email systems will always take place in accordance with Data protection legislation and in line with other policies, including: Confidentiality and the AUP.
 - 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.
 - Organisation email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the Youth Works Northamptonshire community will immediately tell the Designated Safeguarding Lead if they receive offensive communication, and this will be recorded in the organisation's safeguarding files/records.

7.8.1 Staff

- The use of personal email addresses by staff for any official Youth Works Northamptonshire business is not permitted.
 - All members of staff are provided with a specific college email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and students and parents or other service users.

7.8.2 Students

- Students will use college provided email accounts for educational purposes.
- Students will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9 Management of Learning Platforms

- Youth Works Community College uses Moodle as its official learning platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular, message and communication tools and publishing facilities.
- Only current members of staff and students will have access to the LP. When staff and/or students' leave the college, their account or rights to specific college areas will be disabled.
- Students 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:
 - The user will be asked to remove any material deemed to be inappropriate or offensive.
 - If the user does not comply, the material will be removed by the site administrator.
 - Access to the LP for the user may be suspended.
 - The user will need to discuss the issues with a member of leadership before reinstatement.
 - In the case of inappropriate use by students, parents/carers may be informed.
 - If the content is considered to be illegal, then the college will respond in line with existing child protection procedures.
- Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership team; in this instance, there may be an agreed focus or a limited time slot.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of the Youth Works Northamptonshire 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 the Youth Works Northamptonshire community are expected to engage in social media in a positive, safe and responsible manner, at all times.
 - All members are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The organisation will control access to social media whilst using college provided devices and systems on site through the use of blocking specific sites/apps and age restricted material.
 - The use of social media during college hours for personal use is permitted during break times.
 - Inappropriate or excessive use of social media during college/work hours or whilst using college devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of the Youth Works Northamptonshire community on social media, should be reported to the Chief Executive Officer and will be managed in accordance with our Anti-bullying, Disciplinary, Behaviour and Safeguarding policies.

8.2 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 the AUP.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within college. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- 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):
 - Setting the privacy levels of their personal sites as strictly as they can.
 - Being aware of location sharing services.
 - Opting out of public listings on social networking sites.
 - Logging out of accounts after use.
 - Keeping passwords safe and confidential.

- Ensuring staff do not represent their personal views as that of the college.
- 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 colleges 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 young people 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 in the college.

Communicating with young people and parents and carers

- Staff, volunteers and trustees must give serious consideration as to the appropriateness of accepting 'friend' or 'follow' requests from students, parents/carer and other service users. If you are in any doubt, seek advice from the Chief Executive Officer.
- Staff will not use personal social media accounts to make contact with young people or parents/carers in an 'official' capacity, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Chief Executive Officer.
- Any communication from students and parents received on personal social media accounts must be reported to the organisation's Designated Safeguarding Lead.

8.3 Youth Works Community College Students' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources.
- Any concerns regarding students' use of social media, both at home and at college, will be dealt with in accordance with existing college policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Students 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. Examples could include real/full name, address, mobile or landline phone

numbers, college attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.

- To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
- 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 and report concerns both within college and externally.

8.4 Official Use of Social Media

Youth Works Northamptonshire's official social media channels are:

- Twitter @Youth_Works
 - Facebook @youthworksnorthamptonshire
 - Instagram @youth_works_northamptonshire
- The official use of social media sites, by the organisation, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
 - The official use of social media as a communication tool has been formally risk assessed and approved by the Chief Executive Officer.
 - Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence.
 - Official organisation social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
 - Staff use college provided email addresses to register for and manage any official college social media channels.
 - Official social media sites are suitably protected and, where possible, linked to and from the organisation's website.
 - Public communications on behalf of the organisation 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, Data protection, Confidentiality and Safeguarding.
 - All communication on official social media platforms will be clear, transparent and open to scrutiny.

- Parents, carers and young people will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Parents and carers will be informed of any official social media use with young people and written parental consent will be obtained, as required.

Staff expectations

- If members of staff are participating in online social media activity as part of their capacity as an employee of the organisation, they will:
 - Sign the organisation's AUP.
 - Be professional at all times and aware that they are an ambassador for the organisation.
 - Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of the organisation.
 - Be responsible, credible, fair and honest at all times 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 written consent before posting images on the official social media channel.
 - Not disclose information, make commitments or engage in activities on behalf of the college unless they are authorised to do so.
 - Not engage with any direct or private messaging with current students, service users, parents and carers.
 - Inform their line manager, the Designated Safeguarding Lead and/or the Head Teacher of any concerns, such as criticism, inappropriate content or contact from students or other service users.

9. Use of Personal Devices and Mobile Phones

- Youth Works Northamptonshire recognises that personal communication through mobile technologies is an accepted part of everyday life for young people, staff and parents/carers, but technologies need to be used safely and appropriately.

9.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate college policies, including, but not limited to: Anti-bullying, Behaviour and Safeguarding.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.

- All members of Youth Works Northamptonshire community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the organisation accepts no responsibility for the loss, theft or damage of such items on their premises.
- All members of the Youth Works Northamptonshire 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.
- The sending of abusive or inappropriate messages/ 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 Youth Works Northamptonshire community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the Behaviour or Safeguarding policies.

9.2 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 organisational policy and procedures, such as: Confidentiality, Safeguarding, Data Protection and Acceptable use.
- Staff will be advised to:
 - Keep mobile phones and personal devices in a safe and secure place.
 - Keep mobile phones and personal devices switched off or switched to 'silent' mode during working hours unless otherwise agreed by their Line Manager.
 - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during working hours.
 - Ensure that any content bought 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 students, service users or parents and carers.
 - Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead and/or Chief Executive Officer.
- If a member of staff breaches the organisation's policy, action will be taken in line with the Disciplinary 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.

9.3 Youth Works Community College Students' Use of Personal Devices and Mobile Phones

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Youth Works Community College expects pupil's personal devices and mobile phones to be switched off or switched onto 'silent mode' and kept out of sight during lessons.
- If a student needs to contact his/her parents or carers they will be allowed to use the office/reception phone.
 - Parents are advised to contact their child via the college during college hours; exceptions may be permitted on a case-by-case basis, as approved by the Head Teacher.
- Mobile phones or personal devices will not be used by students during lessons or formal college 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.
- Mobile phones and personal devices must not be taken into examinations.
 - Students 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 student's withdrawal from either that examination or all examinations.
- If a student breaches the policy, the phone or device will be confiscated and will be held in a secure place.
 - College staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the organisation's 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 the organisation's Behaviour policy.
 - Students' mobile phones or devices may be searched by a member of the leadership team, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes college policies.
 - Mobile phones and devices that have been confiscated will be released to the student at the end of the day.
 - If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation. (www.gov.uk/government/publications/searching-screening-and-confiscation)

9.4 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 the organisation's Acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour and Safeguarding.
- The Designated Safeguarding Lead will ensure appropriate signage and information is displayed 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 Designated Safeguarding Lead of any breaches of organisation's policy.

9.5 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with students or parents/ carers is required.
- Mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- College mobile phones and devices will always be used in accordance with the Acceptable use policy.

10. Responding to Online Safety Incidents and Concerns

- All members of the Youth Works Northamptonshire 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 organisation procedures for reporting concerns.
 - Students, parents and staff will be informed of Youth Works Northamptonshire's complaints procedure and staff will be made aware of the whistleblowing procedure.
- Youth Works Northamptonshire requires staff, parents, carers and young people to work in partnership to resolve online safety issues.
- After any investigations are completed, the organisation will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the Senior Leadership Team are unsure how to proceed with an incident or concern, the DSL will seek advice from the Multi Agency Safeguarding Hub.
- Where there is suspicion that illegal activity has taken place, the college will contact Northamptonshire Police using 101, or 999 if there is immediate danger or risk of harm.

- If an incident or concern needs to be passed beyond the college community (for example if other local colleges are involved or the public may be at risk), the DSL will speak with Northamptonshire Police and/or the Multi Agency Safeguarding Hub first, to ensure that potential investigations are not compromised.

10.1 Concerns about the Welfare of Young People

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
 - The DSL will record these issues in line with the organisation's Safeguarding policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Northamptonshire Safeguarding Children Board thresholds and procedures.
- A member of the organisation's staff will inform parents and carers of any incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Chief Executive Officer, according to the Disciplinary 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 the Disciplinary policy.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Youth Produced Sexual Imagery or "Sexting"

- Youth Works Northamptonshire recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The organisation will follow the advice as set out in the non-statutory UKCCIS guidance: ['Sexting in colleges and colleges: responding to incidents and safeguarding young people'](#).
- Youth Works Northamptonshire will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods including classroom activities and information displays.
- The organisation will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

11.1.1 Dealing with 'Sexting'

- If the organisation is made aware of an incident involving the creation or distribution of youth produced sexual imagery, the organisation will:
 - Act in accordance with our Safeguarding policy and the relevant Northamptonshire Safeguarding Child Board's procedures.
 - Immediately notify the Designated Safeguarding Lead.
 - Store the device securely.
 - If an indecent image has been taken or shared on the organisation's network or devices, the organisation will take action to block access to all users and isolate the image.
 - Carry out a risk assessment which considers any vulnerability of young people involved; including carrying out relevant checks with other agencies.
 - Inform parents and carers, if appropriate, about the incident and how it is being managed.
 - Make a referral to Specialist Children's Services and/or the Police, as appropriate.
 - Provide the necessary safeguards and support for young people, such as offering counselling.
 - Implement appropriate sanctions in accordance with the organisation's Behaviour policy, but taking care not to further traumatise victims where possible.
 - Consider the deletion of images in accordance with the UKCCIS: ['Sexting in colleges and colleges: responding to incidents and safeguarding young people'](#) guidance.
 - Images will only be deleted once the organisation 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 procedures, where necessary.
- The organisation will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off our premises, using college or personal equipment.
- The organisation will not:
 - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
 - In this case, the image will only be viewed by the Designated Safeguarding Lead 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 children (i.e. youth produced sexual imagery) and will not allow or request young people to do so.

11.2 Online Child Sexual Abuse and Exploitation

- Youth Works Northamptonshire 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.
- Youth Works Northamptonshire recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The organisation will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for young people, staff and parents/carers.
- The organisation will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.
- The organisation will ensure that the 'Click CEOP' report button is visible and available to Youth Works Community College students and other members of the college community on the College's Learning Platform. It will also be visible and available on the organisation's website.

11.2. 1 Dealing with Online Child Sexual Abuse and Exploitation

- If the organisation is made aware of an incident involving online sexual abuse of a child, the organisation will:
 - Act in accordance with the Safeguarding policy and the relevant Northamptonshire Safeguarding Child Board's procedures.
 - Immediately notify the Designated Safeguarding Lead.
 - Store any devices involved securely.
 - Immediately inform Northamptonshire police via 101 (or 999 if a child is at immediate risk)
 - Carry out a risk assessment which considers any vulnerabilities of young people involved (including carrying out relevant checks with other agencies).
 - Inform parents/carers about the incident and how it is being managed.
 - Make a referral to Specialist Children's Services (if required/ appropriate).
 - Provide the necessary safeguards and support for young people, such as, offering counselling.
 - Review the handling of any incidents to ensure that best practice is implemented; the leadership team will review and update any procedures, where necessary.

- Youth Works Northamptonshire will take action regarding online child sexual abuse, regardless of whether the incident took place on/off our premises, using the organisation's or personal equipment.
 - Where possible young people will be involved in decision making and if appropriate, will be empowered to report concerns via Click CEOP www.ceop.police.uk/safety-centre/
- If the Leadership Team is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Multi Agency Safeguarding Hub and/or Northamptonshire Police.
- If the organisation is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the [RISE](#) unit by the Designated Safeguarding Lead.

11.3 Indecent Images of Children (IIOC)

- Youth Works Northamptonshire will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- Youth Works Northamptonshire will take action regarding IIOC on the organisation's equipment and/or personal equipment, even if access took place off site.
- The organisation will take action 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 the organisation is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Northamptonshire Police and/or the Multi Agency Safeguarding Hub.
- If made aware of IIOC, the organisation will:
 - Act in accordance with the Safeguarding policy and the relevant Northamptonshire Safeguarding Child Boards procedures.
 - Immediately notify the Designated Safeguard Lead.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Northamptonshire police or the LADO.
- If made aware that a member of staff or a young person has been inadvertently exposed to indecent images of children whilst using the internet, the organisation will:
 - Ensure that the Designated Safeguard Lead 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 organisation's devices, Youth Works Northamptonshire will:
 - Ensure that the Designated Safeguard Lead 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 children's social services (as appropriate).
 - 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 the organisation's devices, the organisation will:
 - Ensure that the Chief Executive Officer is informed.
 - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the colleges managing allegations policy.
 - Quarantine any devices until police advice has been sought.

11.4 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Youth Works Northamptonshire.
- Full details of how the organisation will respond to cyberbullying are set out in the Anti-bullying policy.

11.5 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Youth Works Northamptonshire 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 organisation policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the Leadership Team are unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain

advice through the Multi Agency Safeguarding Hub and/or Northamptonshire Police.

11.6 Online Radicalisation and Extremism

- Youth Works Northamptonshire will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet on site.
- If the college is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Safeguarding policy.
- If the organisation is concerned that a member of staff may be at risk of radicalisation online, the Chief Executive Officer will be informed immediately and action will be taken in line with the Safeguarding and Disciplinary policies.

12. Useful Links

Youth Works Northamptonshire Senior/Deputy Designated Lead
01536 519169 / 01536 518339 / 07479970494

Northamptonshire MASH (Multi Agency Safeguarding Hub)

Tel no: 0300 126 1000
Put of Hours 01604 626938
Email: cypsnccinitialcontact@northamptonshire.gcsx.gov.uk
Web Site: www.northamptonshire.gov.uk/ctps

Northamptonshire Safeguarding Children Board:

- <http://www.northamptonshirescb.org.uk/>

Northamptonshire Police:

- <http://www.northants.police.uk/>
- In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Northamptonshire Police via 101

National Links and Resources

- 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
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for colleges: www.360safe.org.uk

Youth Works Northamptonshire thank Kent County Council for their exemplar online safety policy, on which this policy has been based.

Ratified by the Board of Trustees: 6 September 2019

Review due: 5 September 2020