City College Peterborough

Working together, learning together

Online Safety Policy

Online Safety Lead: Racheal Franklin

1. Contents

City College Peterborough Online Safety Policy

1. Policy aims

- This online safety policy has been written by City College Peterborough.
- It takes into account the DfE (Department for Education) statutory guidance 'Keeping Children Safe in Education' 2021, 'Working Together to Safeguard Children' 2018.
- The purpose of City College Peterborough online safety policy is to:
    - safeguard and promote the welfare of all members of City College Peterborough community online
    - identify approaches to educate and raise awareness of online safety throughout our 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 follow when responding to online safety concerns.
- City College Peterborough 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

- City College Peterborough recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and supported people, and staff are protected from potential harm online.
- City College Peterborough identifies that the internet and associated devices, such as computers, tablets, mobile phones, and games consoles are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks.
- City College Peterborough will empower our learners and supported people to acquire the knowledge needed to use the internet and technology in a safe, considered, and respectful way, and develop their resilience so they can manage and respond to online risks.
- This policy applies to all staff, including the governing body, executive leadership team, tutors, 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, supported people and parents/ carers.
- This policy applies to all access to the internet and use of technology, including mobile technology, or where learners and supported people, staff or other individuals have been provided with setting issued devices for use, both on and off-site.

2.1 Links with other policies and practices

- This policy links with several other policies, practices, and action plans, including but not limited to:
    - Anti-bullying and harassment policy
    - Sexual Violence and Sexual Harassment Policy
    - Acceptable Use of technology Policy (AUP) and/or the Code of conduct/staff behaviour policy
    - Behaviour and discipline policy
    - Safeguarding and Child Protection Policy
    - Confidentiality policy
    - Curriculum policies

- Data Protection Policy.

3. Monitoring and review

- Technology evolves and changes rapidly; as such City College Peterborough will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection, and adults at risk concerns and/or any changes to our 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 Designated safeguarding lead (DSL) will be informed of online safety concerns, as appropriate.
- The named governor/DSL for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.
- Any issues identified via monitoring policy compliance will be incorporated into our action planning.

4. Roles and Responsibilities

- The DSL is recognised as holding overall lead responsibility for online safety.
- City College Peterborough recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Create a whole setting culture that incorporates online safety throughout all elements of college life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer / child on child abuse, use of social media and mobile technology.
- Work with technical staff and IT support to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners and supported people and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all learners and supported people to develop an appropriate understanding of online safety.

4.2 The Designated Safeguarding Lead (DSL), Deputy Designated Safeguarding Leads and Designated Persons will:

- Act as a named point of contact within the setting on all online safeguarding issues.

- Liaise with other members of staff, such as Wellbeing support staff and IT technicians, on matters of online safety.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.
- Work alongside staff to ensure online safety is recognised as part of the settings safeguarding responsibilities, and that a coordinated whole college approach is implemented.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep learners and supported people safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners and supported people with SEN (Special Educational Needs) and disabilities (SEND) face online.
- Ensure all members of staff receive regular, up-to-date, and appropriate online safety training and information as part of their induction and child protection and adults at risk training.
- 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 and college policies and procedures.
- Report online safety concerns, as appropriate, to IT 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.

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

- Contribute to the development of our online safety policy.
- Read and adhere to our online safety policy and acceptable use of technology policy.
- Take responsibility for the security of IT systems and the electronic data they use or have access to.
- Model good practice when using technology with learners and supported people.
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum and Day Opportunities delivery wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the learners and supported people in their care.
- Identify online safety concerns and take appropriate action by following the college safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to a Designated Person and signposting learners and supported people and parents/carers 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 college leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures including Sophos XG 230, military grade filtering service, as directed by the leadership team to ensure that the settings IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL and/or deputies to enable them to take appropriate safeguarding action when required.

4.5 It is the responsibility of learners and supported people (at a level that is appropriate to their individual ability) to:

- Engage in age/ability appropriate online safety education.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use of technology and behaviour policies.
- Respect the feelings and rights of others, on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.
- Seek help from a staff member, if they are concerned about anything, they or others experience online.

5. Education and engagement approaches

5.1 Education and engagement with learners and supported people

- The setting will establish and embed a whole college culture and will raise awareness and promote safe and responsible internet use amongst learners and supported people by:
    - ensuring our curriculum and whole college approach is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance.
    - ensuring online safety is addressed across the curriculum.
    - reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site.
    - creating a safe environment in which all learners and supported people feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
    - involving a Designated Person/Deputy DSL/DSL as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any learners and supported people who may be impacted by the content.
    - making informed decisions to ensure that any educational resources used are appropriate for our learners and supported people.

- City College Peterborough will support learners and supported people to understand and follow our acceptable use policies in a way which suits their ability by:
    - displaying acceptable use posters in all rooms with internet access.

- informing learners and supported people that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
- seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

- City College Peterborough will ensure learners and supported people develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their ability by:
  - ensuring age-appropriate education regarding safe and responsible use precedes internet access.
  - teaching learners and supported people to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid, or acceptable.
  - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval, and evaluation.
  - enabling them to understand what acceptable and unacceptable online behaviour looks like.
  - preparing them to identify possible online risks and make informed decisions about how to act and respond.
  - ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2 Vulnerable Learners and supported people

- City College Peterborough recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage, and personal circumstances. However, there are some learners and supported people, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.
- City College Peterborough will ensure that differentiated and appropriate online safety education, access, and support is provided to vulnerable learners and supported people via visual prompts and the opportunity to participate in courses and certificate surrounding E-Safety.
- Staff at City College Peterborough will seek input from specialist staff as appropriate, including a designated person/Deputy DSL/DSL, to ensure that the policy and curriculum is appropriate to our community's needs.

5.3 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 which is integrated, aligned, and considered as part of our overarching safeguarding approach.
  - as part of existing safeguarding and child protection and adults at risk training/updates or within separate or specific online safety sessions.
  - Staff training covers the potential risks posed to learners and supported people (content, contact and conduct) as well as our professional practice expectations.
  - build on existing expertise by providing opportunities for staff to contribute to and shape our online safety approaches, including curriculum, 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, including personal use of social media, can have an impact on their professional role and reputation.
- make educational resources and tools available for staff to use with learners and supported people such as Harmful online challenges and online hoaxes' as advised by the DfE.
- ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving learners and supported people, colleagues, or other members of the community.

5.4 Awareness and engagement with parents and carers

- City College Peterborough recognises that parents and carers have an essential role to play in enabling young people and adults with care and support needs 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.
  - drawing their attention to our online safety policy and expectations in our newsletters and other external communication (such as letters and social media channels) as well as in our prospectus and on our website.

5.5 Remote Learning:

- City College Peterborough will deliver learning remotely set-up over digital education platform Microsoft Teams.
- Where education and Day Opportunities support is taking place remotely, it is important for staff, learners, and supported people to maintain professional practice as much as possible. When communicating online with parents/carers, learners and supported people, City College staff will:
  - communicate within college hours as much as possible (unless agreed with an ELT/OLT member)
  - communicate through the college channels approved by the senior leadership team. Specific approval from an ELT member is required for any communication via What's App, Facebook Messenger, and similar channels, and must be to meet a specific need that is documented and cannot be met through Teams)
  - use college email accounts (not personal ones)
  - use college devices over personal devices wherever possible
  - not share personal information
  - follow City College Peterborough Code of Conduct
  - follow City College Peterborough Safeguarding and Child Protection Policy procedures.
- If something is seen or heard online that causes concern, or a learner or supported person makes a disclosure of abuse during a phone call, online session, or email, follow the usual Safeguarding procedures, contacting a Designated Person and log a concern on MyConcern. If there is a risk of immediate harm to a child, young person or supported person, call 999.
- City College Peterborough staff will emphasise the importance of a safe online environment and encourage parents and carers to set age-appropriate parental controls on digital devices and use internet filters to block malicious websites. These are usually free, but often need to be turned on.
- The following resources offer support to parents and carers:
  - Thinkuknow provides advice from the National Crime Agency (NCA) on staying safe online

- Parent info is a collaboration between Parentzone and the NCA providing support and guidance for parents from leading experts and organisations
- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Internet matters provides age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- London Grid for Learning has support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Net-aware has support for parents and carers from the NSPCC, including a guide to social networks, apps, and games
- Let's Talk About It has advice for parents and carers to keep children safe from online radicalisation
- UK Safer Internet Centre has tips, advice, guides, and other resources to help keep children safe online, including parental controls offered by home internet providers and safety tools on social networks and other online.

- Microsoft Teams Operation for staff when communicating with parents/carers, learners or supported people:
  - If you are using a webcam, ensure your surroundings do not divulge any personal details. For example, are any noticeboards in view or personal photographs? Sit against a neutral background, blur your background, or apply a background option from Teams.
  - Be aware of your surroundings, especially if sharing confidential or sensitive information.
  - Staff – work wear, no pyjamas.
  - Learners / Supported people – appropriate clothing, no pyjamas.
  - Double check that any other tabs that are open in their browser would be appropriate for a learner / supported person to see, when sharing their screen.
  - Use professional language.
  - Computers and laptops to be used in appropriate areas, not in bedrooms. If a bedroom is your only available workspace, apply a background.
  - Consider activities carefully when planning – online access at our sites has internet content filtering systems in place that are unlikely to be replicated in the home environment.
  - Be careful that staff and learners do not incur surprising costs, e.g., mobile data access charges - (video utilises significant amounts of data).
  - Be clear about whether it is being recorded or if acceptable for learners to record events and expectations/restrictions about onward sharing.

6. Reducing Online Risks

- City College Peterborough 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 their use in the college is permitted
  - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate

- recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and as such identify clear procedures to follow if breaches or concerns arise.

- 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. This is clearly outlined in our acceptable use of technology policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 PREVENT

- City College recognises that terrorist organisations, such as ISIL, are trying to radicalise and recruit people through an extensive use of social media and the internet.
- As with other online harms, City College are aware of the risks posed by the online activity of extremist and terrorist groups. Concerns will be approached in the same way as safeguarding children, learners, and supported people from any other online abuse by following City College safeguarding procedures.

7.2 Classroom use

- City College Peterborough uses a wide range of technology. This includes access to:
  - Computers, laptops, tablets, and other digital devices
  - Internet, which may include search engines and educational websites
  - Learning platform/intranet
  - Email.
- All setting owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place.
  - Sign out procedure. All data on devices to be remove by user if needed and saved to a safe location. Device cleared once returned to IT.
- 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 appropriate search tools as identified following an informed risk assessment.
  - Set to force safe search with Bing and Google and refuse any other search site through firewall.
- We will ensure that the use of internet-derived materials, by staff and learners and supported people complies with copyright law and acknowledge the source of information.
- Supervision of internet access and technology use will be appropriate to learners' and supported peoples' age and ability.

7.3 Managing internet access

- All staff, learners and supported people and visitors will read and agree an acceptable use policy before being given access to our computer system, IT resources or the internet. Disclosure agreement for WIFI implemented.

7.4 Filtering and monitoring

- A guide for education settings and filtering providers: Safer internet guide and resource

https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring

7.4.1 Decision making

- City College Peterborough governors and leaders have ensured that our college has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks.
- 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.
- The governors and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners and supported people; effective classroom management and regular education about safe and responsible use is essential.

7.4.2 Appropriate filtering

- City College Peterborough's education broadband connectivity is provided through <*Ja.net East of England network*>.
- City College Peterborough uses *Sophos XG 230 firewall.*
    - *Sophos Firewall* blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content, and violent material.
    - *Sophos XG 230* is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
    - *Sophos XG 230* integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'.
- We work with *Sophos* to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If learners and supported people or staff discover unsuitable sites or material, they are required to report the concern immediately to a member of staff, report the URL of the site to technical staff/services.
- Filtering breaches will be reported to the DSL (or deputy) and technical staff and will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving learners and supported people.
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or the Child Exploitation and Online Protection Centre.

7.4.3 Appropriate monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - *Firewall - logs and records all internet traffic and builds profile on users for websites visited or attempted to visit. "User Quotient" can set this to email/Notify key users on a number of scenarios*

- 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.
- If a concern is identified via monitoring approaches, we will:
    - Follow college safeguarding procedures, concerns will be responded to a Designated Person, Safeguarding Manager, Deputy DSL or DSL who will respond in line with the child protection and adults at risk policy.

7.4.4 Managing personal data online

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

7.5 Security and management of information systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly. Sophos Intercept X
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use. Moving away from Pen Drive usage offered up OneDrive as an alternative.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments. Rules Block file types. Checked and passed by cyber–Essentials Plus – October 2019.
- Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
- Checking files held on our network, as required and when deemed necessary by leadership staff.
- The appropriate use of user logins and passwords to access our network.
    - Specific user logins and passwords will be enforced for all users.
- 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 have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- All learners and supported people are provided with their own unique username and private passwords to access our systems; learners and supported people are responsible for keeping their password private.
- We require all users to
    - use strong passwords for access into our system.
    - change their passwords every 60 days.
    - not share passwords or login information with others or leave passwords/login details where others can find them.
    - not to login as another user at any time.
    - lock access to devices/systems when not in use.

7.6 Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the 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, learners,' and supported peoples' 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.

7.7 Publishing images and videos online

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

7.8 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 of technology 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. Picked up and monitored by Sophos Antivirus and email filtering service. On click protection checks the legitimacy of a website before showing the user
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email. All email is set to use TLS 1.2 Microsoft Encryption.
- Setting email addresses and other official contact details will not be used to set up personal social media accounts.
- Members of the community will immediately tell a designated person, deputy DSL or the DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

7.8.1 Staff email

- All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.
- 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 supported people and parents.

7.8.2 Learner/supported person email

- Learners and supported people have a username in the form of an email.
- Learners and supported people will agree an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9 Management of learning platforms

- City College Peterborough uses SharePoint as a 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 supported people and parents will have access to the LP.
- Learners and supported people 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.
    - A learner's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing child protection and adults at risk procedures.
- Learners and supported people may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership as part of 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 City College Peterborough 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 City College Peterborough community are expected to engage in social media in a positive and responsible manner.
- All members of City College Peterborough community are advised not to post or share content that may be considered threatening, hurtful, or defamatory to others on any social media service.
- Staff, Learners, and supported people are expected to follow guidelines outlined in the Acceptable Use Policies.
- Concerns regarding the online conduct of any member of City College Peterborough community on social media, will be reported to a designated person, deputy DSL or the DSL and be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection and adults at risk policies.

8.2 Staff personal use of social media

- The safe and responsible use of social media 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 and/or acceptable use of technology policy.

8.2.1 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 college.

    - 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 in accordance with our policies.
- All members of staff are advised to safeguard themselves and their privacy when using social media services. 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 appropriate privacy levels on their personal accounts/sites.
    - Being aware of the implications of using location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Using strong passwords.
    - Ensuring staff do not represent their personal views as being that of the setting.
- Members of staff are encouraged not to identify themselves as employees of City College Peterborough on their personal social networking accounts; this is to prevent information 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. Staff are expected 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 supported 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.

8.2.2 Communicating with learners and supported people and parents/carers

- Staff will not use personal social media accounts to contact learners and supported people or parents/carers, nor should any contact be accepted.
- All members of staff are advised not to communicate with or add any current or past learners and supported people or their family members, as 'friends' on any personal social media sites, applications, or profiles.
- Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL and the Executive Principal.
    - Decisions made and advice provided in these situations will be formally recorded to safeguard learners and supported people, the setting, and members of staff.
- If ongoing contact with learners and supported people 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.
- Any communication from learners and supported people and parents received on personal social media accounts will be reported to the DSL.

8.3 Learners and supported people use of social media

- Safe and appropriate use of social media will be taught to learners and supported people as part of an embedded and progressive education approach via age-appropriate sites and resources.
- Any concerns regarding learners' and supported peoples' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.

- Concerns regarding learners and supported people use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.
- Learners and supported people will be advised:
    - to consider the benefits and risks of sharing personal details or information 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 appropriate adults' permission, and to only do so 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 on social media, both within the setting and externally.

8.4 Official use of social media

- City College Peterborough official social media channels are:
    - *Twitter - CCPboro*
    - *Facebook – CityCollegePeterborough*
    - *Instagram – citycollegepeterborough*
    - *LinkedIn – City College Peterborough*
    - *YouTube – City College Peterborough*
    - *TikTok - City College Peterborough*

- The official use of social media sites by City College Peterborough only takes place with clear educational or community engagement objectives and with specific intended outcomes.
    - 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 accounts for official educational or engagement purposes only.
    - Staff use setting provided email addresses to register for and manage official social media channels.
    - 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 but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection and adults at risk.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent, and open to scrutiny.
- Parents/carers and learners and supported people will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
    - Any official social media activity involving learners and supported people will be moderated if possible.
- Parents and carers will be informed of any official social media use with learners and supported people; 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.

8.4.1 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:
    - Sign our social media acceptable use policy.
    - Be aware they are an ambassador for the setting.
    - Be professional, 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 appropriate consent has been given 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 private/direct messaging with current or past learners and supported people or parents/carers.
    - Inform their line manager, the DSL (or deputy) of any concerns, such as criticism, inappropriate content or contact from learners and supported people.

Please refer to City College Peterborough social media Policy for further information:

https://citycollegepeterboroughac.sharepoint.com/:w:/r/sites/NewHome/Shared%20Documents/Intranet/Staff%20handbook/01%20Induction/Section%205e%20Social%20Media%20Policy%20Dec%2018.docx?d=wac673f14528c4be788a84702dd68f57f&csf=1&web=1&e=j3DMiI&isSPOFile=1

Mobile Technology: Use of Personal Devices and Mobile Phones

- City College Peterborough recognises that personal communication through mobile technologies is part of everyday life for many learners and supported people, staff, and parents/carers. Mobile technology needs to be used safely and appropriately within the setting.

9.1 Expectations

- All use of mobile technology including mobile phones and personal devices such as tablets, games consoles and wearable technology will take place in accordance with our policies, such as anti-bullying, behaviour and child protection and adults at risk and with the law.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - All members of City College Peterborough community are advised to take steps to protect their mobile phones or personal 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 City College Peterborough 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 sites such as changing rooms, toilets, and aqua therapy units.
- 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 in line with our anti-bullying and behaviour policies.
- All members of City College Peterborough 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 and adults at risk 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 policy and procedures, such as confidentiality, child protection and adults at risk, data security and acceptable use of technology.
- Staff will be advised to:
    - keep mobile phones and personal devices in a safe and secure place during lesson and session time.
    - keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson and session 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/support periods unless written permission has been given by ELT such as in emergency circumstances.
    - 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 learners and supported people or parents and carers.
    - Any pre-existing relationships which could undermine this, will be discussed with the DSL.
- Staff will not use personal devices or mobile phones:
    - to take photos or videos of learners and supported people and will only use work-provided equipment for this purpose.
    - directly with learners and supported people and will only use work-provided equipment during lessons/educational/support activities – unless authorised to do so by a member of OLT or ELT.
- If a member of staff breaches our policy, action will be taken in line with our staff code of conduct 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 using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer)/Executive Principal/Chair of Governors will be informed in line with our staff code of conduct and disciplinary policy. A PIPOT (Person in Position of Trust) referral may also be made

9.3 Learners and supported people use of personal devices and mobile phones

- Learners and supported people will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

    - City College Peterborough expects learners and supported people' personal devices and mobile phones to be kept in a secure place, switched off, kept out of sight during lessons and while moving between lessons.
- If a learner needs to contact his/her parents or carers, they will be allowed to use a college phone.
    - Parents are advised to contact their child/cared-for via the college reception; exceptions may be permitted on a case-by-case basis.
- Mobile phones or personal devices will not be used by learners and supported people 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' and supported people 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 and supported people 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 held in a secure place.
    - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection and adults at risk, behaviour, or anti-bullying policy.
    - Learners and supported people mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer (if learner is under 18 or a Power of Attorney is in place). Content may be deleted or requested to be deleted if it contravenes our policies.
    - 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.

9.4 Visitors' use of personal devices and mobile phones

- Appropriate signage and information are provided on display boards to inform parents/carers and visitors of expectations of use.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our acceptable use of technology policy and other associated policies, including but not limited to anti-bullying, behaviour, child protection and adults at risk and image use.
- Members of staff are expected to challenge visitors if they have concerns and inform the DSL (or deputy) of any breaches of our policy.

9. Responding to Online Safety Incidents

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, peer on peer / child on child abuse, including cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.

- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Learners and supported people, 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 and supported people to work in partnership with us to resolve online safety issues.
- After any investigations are completed, leadership staff 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 Service.
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.
- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the DSL will speak with the police and the Education Safeguarding Service first, to ensure that potential criminal or child protection and adults at risk investigations are not compromised.

10.1 Concerns about learner/supported person online behaviour and/or welfare

- A designated person, deputy DSL or the DSL will be informed of all online safety concerns involving safeguarding or child protection and adults at risk risks in line with our child protection and adults at risk policy.
- All concerns about learners' and supported people will be recorded in line with our child protection and adults' at-risk policy i.e., via MyConcern
- City College Peterborough recognises that whilst risks can be posed by unknown individuals or adults' online, learners' and supported people can also abuse their peers; all online child on child (peer on peer) concerns will be responded to in line with our child protection and adults at risk policies.
- A designated person, deputy DSL or the DSL will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be offered to learners and supported people as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required if they are under 18 or Power of Attorney (Care) is in place.

10.2 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the DSL, in accordance with our policies.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer) for staff supporting young people or to the Executive Principal/Chair of Governors for adults.
- Appropriate disciplinary, civil and/or legal action will be taken in accordance with our staff policies.
- Welfare support will be offered to staff as appropriate.

10.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to a designated person, deputy DSL or the DSL. They will respond to concerns in line with existing policies, including but not limited to child protection and adults at risk, anti-bullying, complaints, allegations against staff, acceptable use of technology and behaviour policy.
- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

10. Procedures for Responding to Specific Online Concerns

11.1 Online sexual violence and sexual harassment between children (peer on peer / child on child abuse)

www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals

- Our, DSL, Deputy DSLs', Designated People, and appropriate members of staff have accessed and understood the DfE "Sexual violence and sexual harassment between children in schools and colleges" (Updated Sept 2021) guidance and part 5 of 'Keeping children safe in education' 2021.
    - Full details of our response to peer-on-peer abuse, including sexual violence and harassment can be found in our child protection and adults at risk policy.
- City College Peterborough recognises that sexual violence and sexual harassment between children can take place online. Examples may include:
    - Non-consensual sharing of sexual images and videos (sexting and youth produced sexual imagery)
    - Sexualised online bullying
    - Online coercion and threats
    - 'Upskirting,' which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress, or alarm. It is a criminal offence
    - Unwanted sexual comments and messages on social media
    - Online sexual exploitation
- 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 any concerns relating to online sexual violence and sexual harassment, we will:
    - Immediately notify a designated person, deputy DSL or the DSL and act in accordance with our child protection and adults at risk and anti-bullying policies.
    - Provide the necessary safeguards and support for all learners and supported people involved, such as implementing safety plans, offering advice on blocking, reporting, and removing online content, and 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 referrals to partner agencies.
    - If the concern involves children and young people at a different educational setting, a designated person, deputy DSL or the DSL will work in partnership with other DSLs (Designated Safeguarding Lead) to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, a designated person, deputy DSL or the DSL (or deputy) will discuss this with the 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.

- City College Peterborough 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.
- City College Peterborough recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, City College Peterborough 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 by implementing a range of age and ability appropriate educational methods as part of our curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners and supported people.

11.2 Youth produced sexual imagery ("sexting")

- City College Peterborough recognises youth produced sexual imagery (also known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by a designated person, deputy DSL or the DSL
- We will follow the advice as set out in the non-statutory UKCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people.'
    - Youth produced sexual imagery or 'sexting' is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
    - It is an offence to possess, distribute, show, and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.
- City College Peterborough will ensure that all members of the community are made aware of the potential social, psychological, and criminal consequences of creating or sharing youth produced sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- 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 suspected youth produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so.
    - If it is deemed necessary, the imagery will only be viewed where possible by the DSL, and any decision making will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image/video of a child (i.e., youth produced sexual imagery) and will not allow or request learners and supported people 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 and adults at risk policies and the relevant local procedures.
    - Ensure a designated person, deputy DSL or the DSL responds in line with the UKCIS guidance.
    - Store any devices containing potential youth produced sexual imagery securely
    - If a potentially 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 in line with the UKCIS guidance which considers the age and vulnerability of learners and supported people involved, including the possibility of carrying out relevant checks with other agencies.
- Inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
- Make a referral to Children's Social Work Service and/or the police, as deemed appropriate in line with the UKCIS guidance.
- Provide the necessary safeguards and support for learners and supported people, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCIS 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.

11.3 Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

- City College Peterborough recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by a designated person, deputy DSL or the DSL, in line with our child protection and adults at risk policy.
- City College Peterborough will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target learners and supported people, and understand how to respond to concerns.
- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for learners and supported people, staff, and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
    - Act in accordance with our child protection and adults at risk policies.
    - Store any devices containing evidence securely.
    - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
    - If appropriate, make a referral to Children's/Adults Social Work Service and inform the police via 101, or 999 if a learner or supported person is at immediate risk.
    - Carry out a risk assessment which considers any vulnerabilities of learner(s) or supported people involved, including carrying out relevant checks with other agencies.
    - Inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - Provide the necessary safeguards and support for learners and supported people, such as, offering counselling or pastoral support.
    - 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 abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible and appropriate, learners and supported people will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, a designated person, deputy DSL or the DSL will obtain advice immediately through the Education Safeguarding Service and/or police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by a designated person, deputy DSL or DSL.
- If members of the public or learners and supported people at other settings are believed to have been targeted, a designated person, deputy DSL or the DSL will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- City College Peterborough will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.
- 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 (IWF) block list and by implementing appropriate filtering, firewalls, and anti-spam software.
- If we are unclear if a criminal offence has been committed, a designated person, deputy DSL or the DSL will obtain advice immediately through the police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
    - Act in accordance with our child protection and adults at risk policy.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF) and police.
- 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 IWF 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 IWF via www.iwf.org.uk .
    - Inform the police via 101 or 999 if there is an immediate risk of harm, and Children's Social Work Service, as appropriate.

    - Only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
    - Report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children on college provided devices, we will:
    - Ensure that the DSL is informed in line with our staff code of conduct and / or whistleblowing policy.
    - Inform the Local LADO and other relevant organisations in accordance with our staff code of conduct, Disciplinary and / or whistleblowing policy.
    - Quarantine any devices until police advice has been sought.

11.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at City College Peterborough.

11.6 Online hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at City College Peterborough and will be responded to in line with existing policies, including child protection and adults at risk, 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, a designated person, deputy DSL or the DSL will obtain advice through the Education Safeguarding Service and/or the police.

11.7 Online radicalisation and extremism

- As listed in this policy, we will take all reasonable precautions to ensure that learners and supported people and staff are safe from terrorist and extremist material when accessing the internet on site vis Sophos***.***
- If we are concerned that a learner or adult may be at risk of radicalisation online, a designated person, deputy DSL or the Safeguarding Manager will be informed immediately, and action will be taken in line with our child protection and adults at risk policy.
- If we are concerned that a member of staff may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with the child protection and adults at risk and allegations policies.

Responding to an Online Safety Concern Flowchart

Online Safety Concern

Illegal or Harmful Contact or Conduct

Inform a DP, Deputy DSL or the DSL

Report to agencies, as appropriate and in line with child protection procedure.

This may include CEOP, The Front Door, and/or the police

Key Local Contacts

Designated Safeguarding Lead (s):
Julie Bennett – 01733 293894 Ext: 215

Safeguarding Manager
Racheal Franklin – 01733 882525 Ext: 562

Education Safeguarding Advisor (Online Safety): 03000 415797

Front Door: 03000 411111

LADO: 03000 410888

Police: 101 or 999 if immediate risk of harm

Illegal Content

Accidental Exposure

Deliberate

Child

Member of Staff

Report to DSL

Consult with Education Safeguarding Service

Report to Internet Watch Foundation (www.iwf.org.uk), the police and/or Front Door, as appropriate

Consult with LADO

If criminal or child protection investigation required

Unsure

Consult with Education Safeguarding Service

Possible Internal Actions

- Staff training
- Disciplinary action if deliberate – if member of staff, contact personnel provider
- Internal support e.g. counselling
- Request support/advice from Education Safeguarding Service

Inappropriate Conduct or Content

Conduct

Content

Member of Staff

Child

Report to **Manager/ELT member** in line with allegations

Report to DSL

Report to Internet and/or Filtering Service Provider

Possible Internal Actions

- Sanctions (if deliberate)
- PSHE/citizenship
- Restorative justice
- Anti-bullying
- Parental work
- School support e.g. counselling, peer mentoring
- Request support/advice from Education Safeguarding Service

Record incident, action taken and decision making in line with child protection recording systems. Review policies and procedures and implement changes

Useful Links

Early Help and Preventative Services:

https://fis.peterborough.gov.uk/kb5/peterborough/directory/family.page?familychannel=9

Other:

- Eis - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eisit.uk

National Links and Resources for Settings, Learners and supported people and Parents/carers

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Internet Watch Foundation (IWF): www.iwf.org.uk
- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
  - Report Harmful Content: https://reportharmfulcontent.com/
- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools
- Internet Matters: www.internetmatters.org
- Parent Zone : https://parentzone.org.uk
- Parent Info : https://parentinfo.org

  NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraudé : www.actionfraud.police.uk
- Get Safe Online: www.getsafeonline.org

11. References

- Education for a Connected World Framework
- Peterborough City Council Social Media Policy
- Keeping Children Safe in Education' 2022
- 'Sexting in schools and colleges: responding to incidents and safeguarding young people'
- Sexual violence and sexual harassment between children in schools and colleges
- 'Teaching online safety in school'
- Harmful online challenges and online hoaxes
- Sharing nudes and semi-nudes – advice for education settings working with young people
- Working Together to Safeguard Children' 2018.
- www.ceop.police.uk/safety-centre/
- www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
- www.iwf.org.uk
- www.saferinternet.org.uk/advice-centre/tutortutors-and-school-staff/appropriate-filtering-and-monitoring

Document control sheet

Revision issue date:	05th January 2023
Next Review Due Date:	06th January 2024
Date of most recent Equality Impact Assessment:	19th January 2023
Document Lead and Author:	Racheal Franklin
Approvers and dates:	Governing body
Purpose of the review:	Scheduled review
Dissemination:	MyConcern and website

This document can only be considered valid when viewed via the City College Peterborough internal web pages on the intranet. If this document is printed into hard copy or saved to another location, you must check that the version date on your copy matched that of the intranet version. The date will always appear on the footer.

Revisions	
[insert date]	Additions: • 5.3 - make educational resources and tools available for staff to use with learners and supported people such as Harmful online challenges and online hoaxes' as advised by the DfE. • 7.4.3 - If a concern is identified via monitoring approaches, we will: ○ Follow college safeguarding procedures, concerns will be responded to a Designated Person, Safeguarding Manager, Deputy DSL or DSL who will respond in line with the child protection and adults at risk policy. • Reference to 'child-on-child' abuse added.
	Amendments: Minor changes to terminology e.g. SLT to ELT • page 5 - change the review period to every year • page 9 - replaced college tutors with staff • page 12 - acronyms explained • page 17 – Tiktok added • *page 19* - changed 'staff behaviour and allegations policy' • page 27 - flow chart – box expanded to show all of writing. Contact details updated • References – changes made. Front door service removed as this is for individuals that reside in Kent