ACC ONLINE SAFETY POLICY

Date: November 2021

access
creative college

CONTENTS

The purpose of this policy statement

About us

Access to Music Limited (‘The College’) has subsidiary companies, trading names and trading partnerships through which it operates. The trading names and partnerships might have their own names or brands, but the legal entity for the purpose of this policy is Access to Music Limited, referred to throughout this Policy under its trading name of Access Creative College (ACC).

These include:

- **The provision of learning programmes, including T Levels, for students aged 16+ both in our centres and in work placements.**
- **The provision of apprenticeships.**
- **The provision of traineeships.**

The purpose of this policy statement is to:

- **Ensure the safety and wellbeing of young people and adults is paramount when they are using the internet, social media or mobile devices. (see appendix 1)**
- **Provide staff and volunteers with the overarching principles that guide our approach to online safety.**
- **Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we and our learners use online devices.**

The policy statement applies to all staff, volunteers, young people and anyone involved in the Access Creative College Group’s activity.

This policy should be read in conjunction with the college’s **Safeguarding, Child Protection and Prevent Policy,** its **Staff Code of Conduct** and the separate **ACC Safeguarding and Prevent procedures** guidance for staff.

Legal Framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect young people in England. The legal framework for the role of the ACC Group is based on the range of activities summarised by NSPCC in September 2021 where key legislation for online abuse is identified as follows:

- **Stalking;**
- **Harassment;**
- **Improper use of a public communications network;**
- **Sending indecent, offensive, false or threatening communications;**
- **Sending private sexual photos or videos of another person without their consent.**

The last two bullet points refer to types of abuse which have been reported increasingly as safeguarding cases since the onset of the pandemic and this increase may be partly attributed to the rising use in social media platforms by young people over this period. For this reason, there is a section 'Responding to cases linked to sexting, sexual abuse and sexual exploitation' on **page 4.** In addition to the legal framework defined by the NSPCC and summarised above, the Association of Chief Police Officers (ACPO) provides helpful clarity of their position:

> **'ACPO does not support the prosecution or criminalisation of children for taking indecent images of themselves and sharing them. Being prosecuted through the criminal justice system is likely to be upsetting and distressing for children especially if they are convicted and punished. The label of sex offender that would be applied to a child or young person convicted of such offences is regrettable, unjust and clearly detrimental to their future health and wellbeing.'**

However, there are cases in which children and young people have been convicted and sent to prison. The important thing to remember is that whilst, as a college, we will want to consider the implications of reporting an incident to the police, it is not our responsibility to make decisions about the seriousness of the matter. That responsibility lies with the Police and the CPS, hence the requirement for the college to refer. In summary the sharing of nudes and semi nudes is classed as illegal as it constitutes sharing and/or possessing an indecent image of a child.

Links to the key legislation are itemised in **Appendix 1.** Specific guidance from a number of sources, including statutory requirements, informs our policy and how we implement it. A range of sources are shown in **Appendix 2.**

Policy intent and measures

We believe that…

- Young people should never experience abuse of any kind.
- Young people should be able to use the internet for education and personal. development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that…

- The online world provides everyone with many opportunities; however it can also present risks and challenges.
- The increased use of social media platforms by young people since the start of the Covid-19 pandemic and periods of limited face to face contact have heightened the vulnerabilities and risks faced by learners.
- We have a duty to ensure that all young people and adults involved in our organisation are protected from potential harm online.
- We have a responsibility to help keep young people safe online, whether or not they are using Access Creative College's network and devices
- All learners, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.
- Working in partnership with young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to keep learners safe by:

- Updating this policy as required, for approval by the chair of the Safeguarding and Prevent Committee and the Executive Leadership Team.
- Providing clear and specific directions to staff and volunteers on how to behave online through our staff code of conduct.
- Providing clear guidance on appropriate use of social media platforms or hubs associated with Access Creative College.
- Utilising tutorials, literature and posters to educate young people on identifying potential online safeguarding risks, measures for protecting themselves from these risks, and expected behaviours to protect others; acceptable learner behaviour is enforced by the ACC Learner Disciplinary Policy & Procedure.
- Providing ongoing discussions with the young people using our service about: healthy relationships, abuse and consent, where to go for help and how to report unacceptable activity or behaviour.
- Providing an online safety agreement for use with young people, which all learners must agree to at the start of their studies.
- To develop practices to support and encourage parents and carers to do what they can to keep young people in their care safe online.

- **Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or young person.**
- **Utilising IMPERO (classroom/network management and online safety monitoring software) and other IT systems to monitor and log the use of keywords associated with: adult content, radicalisation, violence, cyberbullying, illegal content, and hate crime targets (LBBTQIA, BAME, religion, etc) on any device accessed on the college network. Reviewing and updating the security of our information systems as appropriate.**
- **Ensuring that usernames, logins, email accounts and passwords are used effectively.**
- **Ensuring personal information about the staff and learners who are involved in our organisation is held securely and shared only as appropriate.**
- **Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given.**
- **Providing supervision, support and training for staff and volunteers about online safety.**
- **Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.**

If online abuse occurs, we will respond to it by:

- **Having clear and robust safeguarding procedures in place for responding to abuse (including online abuse).**
- **Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.**
- **Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account.**
- **Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.**
- **Ensuring that our safeguarding teams manage all cases of suspected or alleged online abuse in line with the principles clearly defined by the UK Council for Internet Safety in their guidance UKCIS guidance.**

Responding to cases linked to sexting, sexual abuse and sexual exploitation:

Sending and sharing ‘nudes and semi nudes’ is one of a number of ‘risk-taking’ behaviours associated with the use of digital devices, social media or the internet. It is accepted that young people experiment and challenge boundaries and therefore the risks associated with online activity can never be completely eliminated. However, Access Creative College takes a proactive approach to help learners to understand, assess, manage and avoid the risks associated with online activity.

We recognise our duty of care to learners who do find themselves involved in such activity as well as our responsibility to report such behaviours where legal or safeguarding boundaries are crossed. It is always our priority to educate learners and support them so that they are aware of activities that are in fact 'criminal' and that through education we help to eliminate these behaviours.

There are a number of definitions of 'nudes and semi nudes' but for the purposes of this policy these are simply defined as:

- **Images or videos generated by children under the age of 18, or of children under the age of 18 that are of a sexual nature or are indecent.**
- **These images are shared between young people and/or adults via a mobile phone, handheld device, computer, 'tablet' or website with people they may not even know.**

There are many different levels of inappropriate 'nudes and semi nudes' and it is likely that no two cases will be the same. It is necessary to carefully consider each case on its own merit. However, it is important that ACC applies a consistent approach when dealing with an incident to help protect young people and the organisation.

For this reason, any such case is reported as a safeguarding case and given immediate attention. The range of contributory factors in each case also needs to be considered in order to determine an appropriate and proportionate response.

The Group is committed to supporting learners who experience any form of sexual abuse including online abuse. All staff are sensitive to the needs of victims and respect their right to be taken seriously. In line with KCSIE (Sept 2021) victims are to be 'kept safe and never made to feel like they are creating a problem for reporting abuse, sexual violence or sexual harassment'.

Staff training

This Online Safety Policy is supported by:

- **The provision of mandatory training to all staff, as part of the CPD programme, covering online safety awareness and their responsibilities in the event of an e-Safety incident.**
- **Refresher activities as deemed necessary to reflect changes made in-year inclusion on the agenda of all team meetings as needed to highlight its importance.**

Related Policies and Procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- **Safeguarding, child protection and Prevent ACC Safeguarding Child Protection & Prevent Policy Procedures for responding to concerns about a child or young person's wellbeing.**
- **Dealing with allegations of abuse made against a child or young person.**
- **Managing allegations against staff and volunteers.**
- **Code of conduct for staff and volunteers.**
- **Learner Disciplinary Policy and Procedure ACC Learner Disciplinary Policy & Procedure.**
- **Photography and image sharing guidance is provided in ACC's Safeguarding, child protection and Prevent procedures document and follows the advice of the UK Council of Internet Safety UKCCIS Advice on 'sexting'.**
- **Social Media Policy.**

Appendix 1

Acts:

- **Computer Misuse Act 1990**
- **Data Protection Act 1998**
- **Malicious Communication Act 1998**
- **Counter-Terrorism and Security Act 2015**
- **The Education Act 2002 - Section 157 & 175**
- **Working together to Safeguard children / young people (2018)**
- **The Mental Capacity Act (2005)**

Summaries of the key legislation and guidance are available on:

- **Online abuse**
- **Bullying**
- **Child protection**
- **Keeping Children Safe in Education - Statutory guidance for schools and colleges on safeguarding children and safer recruitment**
- **Draft Online Safety Bill**

Appendix 2

Keeping Children Safe in Education (September 2021) provides statutory requirements of schools and colleges and ACC's Safeguarding, child protection and Prevent Policy is refreshed annually in line with changes and updated in-year as required.

KCSIE in 2021 introduced the categorisation of four areas of online safety. The 'breadth of issues' within online safety are classified as follows:

- **Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.**
- **Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.**
- **Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and**
- **Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group.**

ACC's Online Safety Policy considers the '4Cs' above while reflecting the fact that many young people have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G).

KCSIE assesses the impact: 'This access means learners while at college can potentiallly sexually harass their peers via their mobile and smart technology, share indecent images: consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content.'

ACC utilises tutorials, **literature** and posters to educate learners on identifying potential online safeguarding risks, measures for protecting themselves from these risks, and expected behaviours to protect others; acceptable learner behaviour is enforced by the ACC Learner Disciplinary Policy & Procedure 2020.

Contact and conduct - Sexual abuse and sexual harassment

The Group has a zero tolerance policy on sexual harassment in whatever form including online and social media, such as 'sexting' and the sharing of unsolicited images.

As part of our safeguarding duties, the Group ensures that learners are made aware that some forms of online activity such as consensual sharing of images and videos are not 'abusive' but are in fact illegal. This is done through a variety of means including regular inputs in group tutorials and the use of posters, such as this learner-facing **Online Safety poster.**

The advice of the UK Council for Internet Safety (UKCIS 2020) is followed by safeguarding teams in ACC in supporting learners from the risks of online abuse and in managing incidents. The ACC Group recognises that teaching young people about safeguarding issues can prevent harm by providing them with the skills, attributes and knowledge they need to identify risks, including those encountered online and to access help when they need it.

The Group actively works to minimise the risk of **peer on peer** abuse by ensuring that all learners are aware that there is a zero-tolerance approach to abuse. In no circumstances is it ever acceptable for abuse to be passed off as 'just banter' or 'just having a laugh'. The ACC Group is committed to countering any culture of unacceptable behaviours and an unsafe environment to learners.

Risks of peer on peer abuse are minimised by ensuring that all members of staff are alert to any signs of it and are confident in challenging unacceptable behaviour immediately and following the college's processes. In line with KCSIE, both victim and perpetrator and any others involved are well supported.

The processes for reporting any incidents or disclosures are documented in 'ACC Safeguarding and Prevent procedures and processes guidance handbook'.

Other sources of guidance:

- **Teaching Online Safety in schools DfE publication includes information useful for support and intervention by post 16 providers.**
- **Impero Online safety handbook - 'A best practice deployment guide and resource pack for Senior Leadership Teams'.**
- **UKCIS publication 'Online safety in schools and colleges Online safety Handbook.**

    - **UK Safer Internet Centre – a partnership between Childnet International, Internet Watch Foundation and SWGfL to promote the safe and responsible use of technology for young people. Their website includes a range of practical resources and support for schools including:**

        - **360 Degree Safe** - a free to use self-review tool for schools to assess their wider online safety policy and practice
        - A Helpline - This helpline was established to support those working with children across the UK with online safety issues. Operated by SWGfL, it can be contacted at 0344 381 4772 and **helpline@saferinternet.org.uk**
        - Safer Internet Day - The UK Safer Internet Centre organise Safer Internet Day for the UK and each year develops a range of materials from assemblies to lesson plans, posters to quizzes, for each key stage, to address a key online safety issue.

- **UK Council for Internet Safety - The UK Council for Internet Safety expands the scope of the UK Council for Child Internet Safety to achieve a safer online experience for all users, particularly groups who suffer disproportionate harms. The website has useful resources for schools and parents to help keep children safe online including:**
  - **Education for a Connected World - a framework describes the Digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it.**
  - **Age specific advice on potential harms and risks can be found in the following sections of the Education for a Connected World framework:**
    - Online relationships
    - Privacy and Security
    - Online reputation
    - Online bullying
    - Self-image and identity
    - Online reputation
    - Online bullying
    - Health, wellbeing and lifestyle

- **Professionals Online Safety Helpline**
- **CEOP Thinkuknow Programme: Online safety education programme from the National Crime Agency's CEOP Command which aims to safeguard children from sexual abuse and exploitation. Education resources and online advice for children aged 4-18, expert and support and professional development for the children's workforce. Signposts to the NCA's Click CEOP service for children to report concerns related to sexual abuse.**
- **UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use, published February 2019.**
- **The Anti-Bullying Alliance - A coalition of organisations and individuals, working together to stop bullying and create safer environments in which children and young people can live, grow, play and learn. Their website includes a range of tools and resources to support schools prevent and tackle cyberbullying.**
- **DotCom Digital - a free resource for schools, created by children with Essex Police and the National Police Chief Council Lead for Internet Intelligence and Investigations, to be launched October 2019. The resource aims to prevent young people becoming victims of online grooming, radicalisation, exploitation and bullying by giving them the confidence to recognise warning signs and reach out to an adult for help.**
- **Internet Matters - a not-for-profit organisation set up to empower parents and carers to keep children safe in the digital world, they also have a dedicated section of their website for professionals which includes resources to support staff training, whole school programmes and policies and a parent pack to help schools engage with parents about online safety.**
- **Internet Watch Foundation - an internet hotline for the public and IT professionals to report potentially criminal online content, including child sexual abuse images online.**

- NSPCC learning - includes a range of safeguarding and child protection teaching resources, advice and training for schools and colleges.
- PSHE Association - the national body for Personal, Social, Health and Economic (PSHE) education. Their programme of study for PSHE education aims to develop skills and attributes such as resilience, self-esteem, risk-management, team working and critical thinking. They also have many guides about how to teach specific topics.
- SWGfL - a charity dedicated to empowering the safe and secure use of technology. Their website includes a range of free resources for schools covering a range of online safety issues, including digital literacy/critical thinking and consequences of sharing and publishing images.

For learners:

- BBC Own It - Support for young people to take control of their online life, including help and advice, skills and inspiration on topics such as friendships and bullying, safety and self-esteem.
- Childline - includes information for pupils on sexting, gaming, grooming, bullying, porn, relationships.
- Get Safe Online - provides advice for young people about online abuse.

For Parents/Carers:

- Parent Zone - offers a range of resources for families, to help them meet the challenges of the digital age, including parent guides on the latest digital trends and platforms.
- Parent Info - from CEOP and Parent Zone, Parent Info is a website for parents covering all of the issues amplified by the internet. It is a free service which helps schools engage parents with expert safety advice, endorsed by the National Crime Agency's CEOP command. This website provides expert information across a range of online harms.
- Internet Matters - a not-for-profit organisation set up to empower parents and carers to keep children safe in the digital world. Their support for parents includes a range of downloadable guides covering subjects such as transition to secondary school, vlogging & live streaming, online gaming and cyberbullying.
- NSPCC - Keeping children safe online Includes a range of resources to help parents keep children safe when they're using the internet, social networks, apps, games and more.
- Thinkuknow - National Crime Agency guide for parents/carers for children and young people of all ages.
- Advice for parents and carers - UK Safer Internet Centre.