

LCC Guidance for ArtForms Staff working in Educational Settings on the Use of Digital Technologies and Social Media

Revised by ArtForms, September 2023

CONTENTS		Page
1.0	Overview	3
	1.1 – Definition of Students	
	1.2 - Adults at Risk	
2.0	Responsibilities	4
3.0	Social Contact with Students, Children or Young People	4
4.0	Social Media	5
5.0	Creating Images of Students through Video or Photography	6
6.0	Use of personal technology/equipment in School	7
7.0	Internet use	8
8.0	Confidentiality and Security	8
9.0	Cyber Bullying	9

Section 1 - Overview

ICT and the internet are essential tools for teaching and learning and communication that are used by ArtForms to deliver the curriculum, and to support and challenge the varied learning needs of its students.

It is important that ArtForms staff use ICT appropriately and practise good online safety when working in educational settings.

E safety covers the use of the internet as well as mobile phones, electronic communications technologies and the use of social media and social networks. We know that some adults will use these technologies to harm students. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. Staff have a duty of care to protect children from risk of harm, as well as a duty to ensure their own conduct does not bring into question their suitability to work with children.

This guidance takes into account the principles of the Safer Working Practice Guidance (National Safer Recruitment Consortium) as well as guidance from the Department for Education (Safeguarding Children in a Digital World), CEOP (Child Exploitation and Online Protection) and Communication Act 2003 (Section 127 Improper Use of Public Electronic Communications Network). <http://www.legislation.gov.uk/ukpga/2003/21/section/127>

This guidance applies to all staff employed either directly or indirectly by ArtForms as well as volunteers and staff not employed directly by ArtForms but working on our behalf. All staff are expected to adhere to this code of practice to ensure the safety of the students, young people and adults at risk who they may come into contact with through their professional role. Any member of staff found to be suspected of any breach of these guidelines may be subject to disciplinary action in accordance with the Schools Disciplinary Policy and Procedure.

1.1 Definition of Students:

Throughout this document references are made to students. For the purpose of this document this term refers to all children, young people and adults at risk in educational settings whom a professional may come into contact with, as a direct result of their professional role.

1.2 Adults at Risk: means adults who need community care services because of mental or other disability, age or illness and who are, or may be unable, to take care of themselves against harm or exploitation. The term replaces “vulnerable adults”.

Section 2 - Responsibilities

The senior leadership team are responsible for ensuring this guidance is shared with and adhered to by all staff.

Staff are responsible for their own actions and must act, and be seen to act, in the best interests of children at all times. Staff must ensure they understand and adhere to this guidance as well as ArtForms' code of conduct. Staff are responsible for acting promptly to prevent and safeguard children from potential abuse online and for reporting any concerns in accordance with the Leeds Childrens Services/ArtForms Safeguarding & Child Protection Policy for Schools and Colleges.

Staff are solely responsible for any content on their own personal social media networks and electronic devices. This means that staff are responsible for managing their own applications and content to ensure that it does not breach Leeds city council's safer working practice guidance, or undermine public confidence in ArtForms or the education profession. Staff are personally responsible for security and privacy settings when using social media via their chosen equipment and as such failing to ensure adequate and appropriate settings are in place may lead to disciplinary action should the content be found to breach ArtForms expectations of professional conduct by bringing ArtForms into disrepute.

Staff are also responsible for ensuring their own use of ICT and social media is professional and appropriate at all times. Staff must be aware that their conduct online, must not breach the council's code of conduct or professional expectations. Any behaviour that is deemed to breach such expectations may be subject to disciplinary action.

Section 3 - Social Contact with Students

Staff must not establish or seek to establish social contact with students, for the purpose of securing a friendship or to pursue or strengthen a relationship. Even if a student themselves seeks to establish social contact. If this occurs coincidentally, the member of staff should exercise their professional judgement in making a response and be aware that such social contact could be misconstrued. Staff should alert the Head of ArtForms of any such contact immediately.

All contact with students should be through appropriate channels at all times and should be within clear and explicit professional boundaries. This means staff should only contact students, regarding ArtForms matters, via parents. Personal email addresses should not be used at any time.

Staff should not give, nor be required to give, their personal details such as home or mobile number, social media identities or personal email addresses to students. Any member of staff found to be in contact with students through any of the above means, or any other unapproved method, without prior consent of the head of ArtForms /senior leader may be subject to disciplinary action.

Section 4 - Social Media

In order to make best use of the many educational and social benefits of new and emerging technologies, pupils need opportunities to use and explore the digital world. Online risks are posed more by behaviours and values than the technology itself.

Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies which detail how new and emerging technologies may be used.

Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat-rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web-cams and other hand-held devices. (Given the ever-changing world of technology it should be noted that this list gives examples only and is not exhaustive.)

Staff should not have contact with students using social media, and specifically social networking sites without prior permission of the Head of ArtForms. Staff must not add students as friends or respond to friend requests from students. If a member of staff suspects that an existing friend is a student, child or young person, they must take reasonable steps to check the identity of the individual and end the social media friendship.

It is recognised that personal access to social networking sites outside the work environment is at the discretion of the individual however members of staff should consider their use of social networks as they take on the responsibilities of a professional, taking particular care to secure personal information and ensure their use of such networking sites is respectable and appropriate at all times.

Secure and suitable strength passwords should be devised and security settings should be applied to access your profile and the information contained within it, so that your profile is limited to those explicitly given access. Users should not sign up to non-work-related web-accounts using a work email address or password.

It is also advisable to log out of any sites on a personal computer or an application on a mobile device to ensure maximum security. Activities undertaken by others who can have access to your social media platforms shall be deemed attributable to the user logged in at the time, unless there is a good and verifiable reason to suspect otherwise (e.g. hacking).

Understand and check your privacy settings on your social media profiles so you can choose to limit who has access to your data. You may also want to consider how much personal information you include on your profile.

Personal profiles on social networking sites and other internet posting forums should not identify your employer or place of work and careful consideration should be given to information which is published on such sites. For example, information which is confidential, damaging to the school or undermines public confidence in the school's reputation.

All postings to social media websites should be considered in the public domain. Therefore, only post comments, videos and pictures which you would be happy to share with any group of friends, strangers or colleagues. Do not post information which could lead to the identification of someone connected to ArtForms or your profession without their explicit consent. This includes posting images of people. Remember once you have published information you cannot guarantee it can be fully removed, and you cannot control how it is shared.

Material published by staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of a student, colleagues or member of the school community will be dealt with under the disciplinary procedure.

Subject to the constraints within this policy it is understood that employees have the right to free expression of opinion in their lives outside school, including on matters of public policy.

Section 5 - Creating Images of Students through Video or Photography

Some work based activities involve recording images and these may be undertaken as part of teaching and rehearsing, for publicity, or to celebrate achievement. However, written explicit consent must be gained from legal guardians prior to creating any images of students.

Using images of students for publicity purposes requires the age-appropriate consent of the individual concerned and their legal guardians. Images should not be displayed on websites, in publications or in a public place without such consent. Consent to use images can be withdrawn at any time, without giving a reason, and in

such cases, staff must make every effort to remove/destroy these images wherever they have been published.

Photograph or video images should be created using equipment provided by the work place. It is not acceptable to record images of students on personal equipment such as personal cameras, mobile phones or video camera without prior consent of the Head of ArtForms. Images of students must not be created or stored for personal use.

Members of staff creating or storing images of students using personal equipment without prior consent will be subject to disciplinary action.

Members of staff must:

- be clear about the purpose of the activity and about what will happen to the photographs when the activity is concluded;
- ensure that senior management is aware that photography/image equipment is being used and for what purpose;
- ensure that all images are available for scrutiny in order to screen for acceptability;
- be able to justify images of students in their possession;
- ensure that images are held only for as long as necessary for the 'purpose'. The recommendation for images of children and young people is that they should only be held for 2 years;
- avoid making images in one to one situations.

Members of staff must not take, display or distribute images of students unless they have explicit written consent to do so. Failure to follow any part of this code of practice may result in disciplinary action being taken.

For further guidance on creating, displaying and storing images of students please refer to the Safer Working Practice Guidance (National Safer Recruitment Consortium 2019) as well as guidance from the Department for Education (Safeguarding Children in a Digital World) and CEOP (Child Exploitation and Online Protection).

Section 6 - Use of personal technology/equipment in schools, music centres and CLYM groups

As peripatetic teachers, there is a need for ArtForms colleagues to access ICT in schools and settings whilst carrying out teaching activities. Examples of this are to access the Eepos teachers' portal to complete registers; to make audio recordings of instrumental/vocal rehearsals and performances; and to access teaching resources, such as backing tracks or other teaching aids. It is best practise to use a school or LCC device, however, there are many occasions when this is not possible, especially

when teaching in areas other than classrooms, and a teacher will need to use their personal device, such as a mobile phone or ipad.

Colleagues taking personal devices into schools must ensure that there is no inappropriate or illegal content on the device. A personal device should always be password protected, ideally with facial recognition. It is recommended to use Wifi when using a mobile device in schools to ensure that devices are covered by firewalls and blocking software. The use of Wifi is at the discretion of schools.

The use of any personal equipment in schools should also be in line with school policies.

It is acknowledged that some schools do not permit the use of personal devices in teaching areas and it may be necessary to seek permission from the Headteacher giving specific examples of the use that is required.

Section 7 - Internet Use

ArtForms colleagues with internet use in a school must follow and adhere to the school policies on the use of IT equipment.

ArtForms colleagues will be issued with a workplace email address and this should be used to communicate with colleagues, schools, settings and parents. Use of this email address must be compatible with colleagues' professional role and may not be used for private purposes, without permission from a member of SLT.

Section 8 - Confidentiality and Security

The storing and processing of personal information is governed by the General Data Protection Regulation and Data Protection Act 2018. Employers are required to provide clear advice to staff about their responsibilities under this legislation so that, when considering sharing confidential information, the principles set out in the legislation apply.

Members of staff may have access to confidential information about students and families and the organisation in order to undertake their everyday responsibilities and in some circumstances this may be highly sensitive or private information. Such information should only be shared when legally permissible to do so and in the interest of the child. Records should only be shared with those who have a legitimate professional need to see them.

Only authorised devices and systems should be used to store and transfer confidential information. Developments in technology have improved the security of email. This has meant that Leeds City Council have been able to follow centrally issued guidance to protect personal and special category data sent by standard email. When email services are configured appropriately at BOTH ends of the route,

email is just as good as Mail Express or any other secure data transfer mechanism once controls are in place.

For further guidance in relation to sending personal information electronically, please refer to the guide for schools – December 2018 titled 'Exchanging data electronically'. Members of staff found to be compromising confidentiality by use of unauthorised systems and devices could be subject to disciplinary action.

For further guidance in relation to confidentiality issues and safe storage of data please refer to the Safer Working Practice guidance document (2019).

Section 9 - Cyber Bullying

All forms of bullying, including cyber bullying, are taken very seriously. Bullying is never tolerated and it is not acceptable for any member of staff to behave in a manner which is intimidating, threatening or in any way discriminatory. Behaviour which constitutes Bullying or Harassment may be dealt with under the Grievance/Bullying and Harassment Policy and could result in disciplinary action.

However, this doesn't just extend to behaviour within the work place. In some instances bullying or harassment that occurs outside the workplace where there is a link to employment could also fall under the responsibility of the employer and therefore result in disciplinary action being taken against the responsible individual.

Certain activities relating to cyber bullying could be considered criminal offences under a range of different laws. Cyber bullying consists of threats, harassment, embarrassment, humiliation, defamation or impersonation and could take the form of general insults, prejudice based bullying or discrimination through a variety of media. Media used could include email, Virtual Learning Environments, chat rooms, web sites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

If an allegation is received that a member of staff is responsible for comments made online which could be deemed harmful, threatening, defamatory, abusive or harassing in any way towards another employee, ArtForms will investigate this matter. Any allegation of bullying or harassment made by an employee against another member of staff where the accused uses the internet, mobile phone, text message or email, along with any other forms of abuse could lead to disciplinary action.

Staff are required to take steps to protect themselves and their personal information by:

- Keeping all passwords secret and protect access to their online accounts
- Not befriending students and young people on social networking services and sites

- Keeping personal phone numbers private
- Not using personal phones to contact parents and students and young people
- Keeping personal phones secure, i.e. through use of a pin code.
- Not posting information about themselves that they wouldn't want employers colleagues, students, young people or parents to see
- Not retaliating to any incident
- Keeping evidence of any incident
- Promptly reporting any incident using existing routes for reporting concerns.

Staff teaching in schools, as well as students, may become targets of cyberbullying. Staff should never retaliate to, i.e. personally engage with, cyberbullying incidents. They should report incidents appropriately and seek support.

Staff should report all incidents to the designated line manager or member of the senior management team. The designated person will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.

For various reasons, staff may find it difficult to report to their line manager in the first instance. They may want additional support or advice. They should know they can seek advice and help from their Union, professional association, from Education Support Partnership, or other organisation.

Further information and advice regarding cyber bullying can be found in the DfE guidance documents Preventing and Tackling Bullying 2017 and Cyberbullying: Advice for Head Teachers and School Staff 2014.

<https://www.gov.uk/government/publications/preventing-and-tackling-bullying>