Paradigm Arts Online Best Practice

This advice and guidance should be read in conjunction with the following policies that govern Paradigm Arts' interaction with children & young people in the delivery of educational activity. All policy and procedural documentation is reviewed annually and/or with the release of new or amended government guidance:

- Online Safety Policy
- Child Protection Policy
- Child Protection Procedural - inc. Cause For Concern Reporting
- Anti-bullying & Cyber Bullying Policy
- Complaints Policy

Whatever the context, the overall aim of any education programme delivered online by Paradigm Arts, is to create the safest possible environment for all our participants.

Paradigm Arts and associate delivery partners have a duty of care to ensure that any online space we create as with the physical opportunities we create, is somewhere that participants can feel safe and comfortable. A place where they are treated equitably and with respect.

Further to this, it is equally important that we also create an online space where they are given the freedom to have fun, developing their independence and creativity.

Although we expect Paradigm Arts' policy and procedural documentation to be followed carefully, staff should also be mindful that every online project and situation is different. Rules, regulations and procedures should always be followed but common sense, experience and sound professional judgement should also be used to anticipate and respond appropriately to different situations. There are, of course, elements of good practice that will help you to minimise risk and create the kind of positive environment described above. It is important to remember that you cannot eliminate risk entirely.

Below are some helpful Do's and Don'ts when interacting with or creating online content:

DOS

- Read the terms and conditions of any sites you sign up to thoroughly. Ensure you are aware of who owns data posted on the site and what the owners of the site can do with your data
- Protect yourself against identity theft by reviewing and customising security settings, checking the site's privacy policy and logging off when you leave a computer or device
- Watch out for suspicious or unusual activity or language from your friends, as this may be a sign that their account has been hijacked.
- Be wary of any request for personal information via a social networking site, especially confidential information such as bank account details
- Think carefully before making any comment relating to your job or employer. Is the information in any way sensitive? Even with privacy settings, content may end up being shared elsewhere

DON'TS

- Do not connect with young people who you work with directly as a client or their carers on social media sites

- Do not publish content that may result in legal action being taken. This includes sharing illegal materials, prohibited images, materials in breach of copyright or discrimination legislation or views that may be considered defamatory

- Do not harass, bully, stalk or otherwise mistreat other employees, volunteers, partners, and/or members of the public

- Do not assume you have made a 'private post'. Information posted online should be considered to be in the public domain, even where security settings have been applied.

How can you minimise the risk to yourself when using social media and electronic communication?

- Manage your privacy settings and keep them under review. This is particularly important regarding photographs.

- Remember that no privacy mechanism is 100% guaranteed;

- ensure your settings prohibit others from tagging you in any photos or updates without your permission and you can ask others to remove any undesirable content related to you;

- consider that conversations held online may not be private. Be aware of who may have access to what you post;

- assume that information you post can be accessed and altered;

- use strong passwords and change them regularly. Protect your mobile phone/smart phone/tablet/computer with a PIN, especially when in schools or working with young people to protect access to its content and potential misuse;
  In the event that you are the victim of cyber bullying or uncomfortable with comments, photos or posts made by participants/colleagues of or about you, bring the matter to the attention of your employer using the proper procedures.

In your day-to-day work there will be instances where you will have to interact with participants online, at all times a professional level of communication is expected.

In order to keep young people safe and to ensure a positive online working environment it is vital that staff, participants, and volunteers, are aware of behaviours that will not be tolerated in our online working environment and community.

For example, the list below, which is by no means exhaustive, is illustrative of the types of behaviours that warrant disciplinary measures and even legal action:

- inappropriate electronic communication with young people, colleagues and parents/carers, including SMS and instant messaging;

- posting/sending sexually explicit pictures/images to colleagues or pupils;

- grooming - whereby a staff member uses electronic messages with a view to establishing an inappropriate relationship with a young person;

- possessing, making, viewing or distributing indecent images of children;

- using inappropriate online content in an educational setting

It is important to understand and follow guidelines that minimise risk when using electronic communication and social networking with young people. Many of these are good practice when working online with any age group. Some examples are listed below.

PARADIGM STAFF staff will:

- always maintain a courteous and professional tone in communicating with young people and ensure that professional boundaries are maintained;

- only use official channels of communication that are agreed and provided by Paradigm Arts e.g. Teams, work e-mail addresses, and be aware of and comply with Paradigm Arts' policies and guidance;

- not exchange private text, phone numbers, personal e-mail addresses or photos of a personal nature with young people;

- firmly decline 'friend' requests from young people and should not send any to young people.

- Use their own discretion when dealing with friend requests from parents/carers/guardians. It is best practice to decline these invitations and remind of the more formal channels which they can discuss their child's engagement with Paradigm Arts' delivered activity;

- not operate online in a way in which would call into question your position as a professional;

- realise that young people may naturally be curious about your personal life outside of and may try to find out more about you.

- Do not discuss participants, colleagues, parents or carers online or criticise your employer;

- Respect young people's privacy and confidentiality at all times;

How can you minimise risk for young people when using electronic communication and social media?

- if you come across or are made aware of the inappropriate use of electronic communication or social networking by a young person or concerning a young person, report the matter to the DSL using the appropriate procedures as outline in Paradigm Arts' Child Protection Policy;

- alert young people you are working with to the Paradigm Arts' Code of Conduct and policies on safe online behaviour, making sure that this is communicated simply, clearly, and effectively.

- be aware of and comply with Paradigm Arts' rules and policy regarding taking and sharing photos or films that include young people that we have worked with. Always follow proper procedure regarding release forms. Good practice is to also double-check the permissions we have before any photos/films/promotional materials go out as not all young people will have the same level of permissions with regards to being filmed/photographed. Anyone over the age of 18 can inform consent for images to be used but anyone under the age of 18 at the point they join a project or activity that could/will lead to material being generated must have a signed document in place from either their legal parent or guardian.

Many of the safeguarding and protection policies that guide you in your day-to-day online work are the same as those that guide you in your face-to-face interactions with young people. If you feel that something is not right then you have a duty to act on it accordingly. Safeguarding children is the responsibility of all and any behaviours that cause you concern for an individuals safety must be communicated effectively and efficiently. It is better to raise a concern than ignore.

In all cases relating to the safeguarding of children and young people you have a responsibility to bring it to the attention of Paradigm Arts' DSL.

The only exception is if your concern relates to them or their actions in which case the following procedures should be implemented.

What to do in an Emergency?
If you are concerned about the immediate safety of a child, for example a child at risk of immediate harm or injury contact the Lincolnshire's Safeguarding Children Partnership 01522 782111 or the police **immediately** do not delay, as this could result in serious injury to a child.

Remote Learning

Paradigm Arts will NEVER ask NOR instruct a young person to engage with remote learning either by providing their own personal communication information or by requesting contact on an individual basis. All communications will be conducted through anonymised email accounts provided to each participant via parents/guardians. Where the young person is over the age of 18 this can be done directly. Young people can share their account information but the data and access to resources will be terminated at the conclusion of every project or suspended if concerns arise relating to use.

If you anticipate the need to record or capture elements of the remote delivered activity permission must be sought from all participants beforehand.

Online consent forms
Online consent/release forms should always be used to record consent for children to take part in activities/programmes. These should be stored in accordance with the Data Protection Act 2018. Parents and carers, and participants aged 16 and over, should be informed of how this information will be stored and used. Young people aged 13 and over should also be asked for their consent for us to store their data.

Things to consider include:

- how you will verify that forms have been signed by the right person (a parent/carer must sign if participants are under 16 years of age)

- how you will keep the forms secure

- how authorised staff will access and check the forms as necessary
- whether all parents and carers will have access to an online system

Livestreaming

Livestreaming can be used to broadcast an event or to view external events. It's a valuable educational medium.

To create a safe environment for young people when watching or engaging in a livestream, there are several things to consider.

Before starting any livestream, remind young people:

- not to share private information
- not to respond to contact requests from people they don't know
- who they should tell if they see or hear anything upsetting or inappropriate

Whether hosting or joining a livestream, you must get consent from parents and carers and young people if any images of or identifying information about a participant will be used. It is best practice to not only include this, where possible in any release forms that participants/parents/carers may have signed but to also remind participants/parents/carers of this BEFORE any livestream takes place.

At times you may engage with a wider audience who may not be signed up to one of our programmes. In this instance you should be mindful that they will likely not be familiar with Paradigm Arts' policies and will not have given certain permissions through the usual channels (release/consent forms, etc). By following further guidelines below for ALL livestreams, regardless of audience type, you should avoid any issues.

When hosting a livestream

- consider which platform to use since free platforms such as YouTube or Facebook Live do not allow you to restrict the audience.
- consider inviting your audience to register to watch the stream and issue a log in and password, or look into using a custom platform if you're livestreaming regularly.
- familiarise yourself with the privacy settings and know how to report any offensive or abusive content
- the stream should take place at appropriate times and must be supervised by appropriate adults at all times
- be sensitive to the needs of individual participants, including d/Deaf and disabled children, and children who may be sensitive to certain topics or issues that may arise during the livestream

- appropriate staff should supervise and be on hand to handle any sudden changes or upsetting developments that may occur during the livestream.

You can also involve parents and carers by:

- sharing resources, news activities and events via social media, newsletters, handouts and email
- circulating new and updated e-safety policies and procedures
- organising and inviting parents to online safety sessions, potentially using external visitors

Other resources that give advice to participants about staying safe online:

- BBC Own It – advice and information for children by children about online life
- ThinkUKnow – advice & animations for children about staying safe on a phone, tablet or computer – by National Crime Agency
- Staying Safe Online – advice for parents on steps to take to keep children and teenagers safe online – by Scottish Government
- Get safe online - the UK's leading source of unbiased, factual and easy-to-understand information on online safety.