online safety and ICT policy

Randstad takes its responsibility seriously for the safety of all those using online platforms to receive and deliver education. Pupils, teachers/tutors, parents/carers, commissioning bodies and Randstad are all actively responsible for playing a role in ensuring online safety of children in a virtual/ remote learning environment.

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Randstad safeguarding policy.

All our online sessions are recorded either in our own platform, Bramble, or within a schools own designated platform. These sessions are recorded to ensure spot audits can be conducted to monitor quality and any potential safeguarding concerns. Consent will be sought from all parties before these sessions take place and confirmation of parent's/carer's attendance is confirmed at the outset of the session by the tutor.

online tuition

Tutors conducting tuition on Bramble or any other school verified platforms must adhere to the following:

- Tutors are to only have contact with pupils/parents through the Company platform (Bramble). Any contact outside of tutoring time must be with the school or parents rather than with the pupil directly.
- Should a school wish to use a different video conferencing platform to the Company default, Randstad will get the school to confirm via a google consent form.
- Sessions will be recorded and audited at random to review quality and potential safeguarding.
- From time to time, Randstad or the school may conduct drop-ins to sessions.
- Check the correct pupils/parents are invited to the session and that they have agreed to tutoring before sessions begin.
- Clear guidance will be provided to the parent or guardian of the expectations of them, their child and the tutor.
- Contact details of a randstad representative and the designated safeguard lead will be provided to the parent or guardian to support the reporting of any safeguarding concerns at any point during the provision of online tuition
- Pupil attendance and/or non-attendance must be recorded and notified to randstad.

- For primary school pupils, the parent/carer must be in the room to supervise tuition when tutoring is done online.

- For secondary school pupils, the parent/carer should be within earshot (for example in the next room with the door open) to supervise pupils when tutoring is done online.

- Any safeguarding concerns must be notified to Randstad immediately.

- Any requests for sessions out of school hours (evenings/weekends) must be approved in advance to ensure appropriate supervision can be put in place where needed.

- Ensure you have a complex password to access the system: This means having a mixture of numbers,letters, capitals, and possibly special characters.

- Do not share your login credentials with others. No other members of the household should know or can guess your password(s). If passwords are written down (which should be a last case scenario) they must be stored securely (e.g., in a locked drawer or in a secure password protected database). Passwords should never be left on display for others to see.

- Avoid accessing video facilities on a mobile phone: as well as being impractical (as you may not be able to see all users on a mobile device), there have been instances of video conferencing software sharing data with social media channels (such as Facebook) without permission.

- Check all the correct participants are present on the video call: It can be possible for unauthorised users to join video calls. It may be best to start the call with a register if many users are involved on the call.

- Ensure settings are fixed so that other users on the call cannot record the conversation covertly: Check the system's settings to ensure that other users can't record calls. Also remind users at the beginning that they should not record the call.

- External links shouldn't be shared: Video conferencing isn't always encrypted and so can be vulnerable to unauthorised users who can join calls and send links to others (and these links when opened may expose user's account details). At the beginning of a call, it may be beneficial to remind users not to open any external links sent over chat.

- Sensitive documents shouldn't be shared over video call: Screen share facilities should be used rarely and should contain no personal data where possible. Other users may take a screenshot and then have a copy of data they may not be entitled to.

- Take control of the meeting: It is always best to be the facilitator and run the meeting, set the ground rules (such as making it clear there is to be no recording) and also to set rules on chat etiquette (such as asking users to raise their hand before speaking).

- Limit sending private or "side" messages to users: Content should be available to all.

- Preparation/follow up: If you need to send documents or work in advance or following a session, do ensure that (1) all users are blind copied (BCC) into the email and (2) to avoid sending any sensitive data (such as health data) in those emails. If you need to send sensitive data to a specific individual, do re- check the email address before sending to check it is being sent to the correct recipient.

- Do not give out personal email addresses and numbers to users. Providing personal details such as phone numbers, social media accounts or email addresses are forbidden in any circumstances. Please ensure you only provide them with official work communications only and email address if provided with one by a school.

- Do report any behavioural or safeguarding concerns to Randstad immediately.

- Be careful of what is on display in your background. Remove any material which could be construed as inappropriate or offensive. If you are unsure, it is best to blur your background.

- Tutors must ensure they are appropriately dressed to conduct sessions with pupils.

ICT usage

When utilising ICT equipment in homes etc, we advise that you follow some simple rules:

- Try and organise access to the network with your own username and password. Try to avoid using another person's 'login'.

- Do not use computers for personal use. It reflects badly on you and us if you are observed undertaking such activities.

- If you are using the internet ensure that the sites you visit are always relevant and appropriate. If

you inadvertently visit a site that has inappropriate material displayed, immediately close down the site and report to a senior member of staff.

- Do not let pupils or other staff use your 'login' details and always 'log off' if your computer is going to be left unattended at any time.

- If you suspect pupils/young people or carers have used a computer with your login credentials, report it.

- If you have reason to send emails, ensure that the language you use is always appropriate. Check what you are writing to make sure that it could not be misconstrued.

- Never enter into over-familiar correspondence with pupils/young people. Remember that you are in a position of trust. If you receive any email correspondence from a pupil that concerns you please report this immediately.

- Never give a pupil/young person your mobile phone number. Similarly, do not ask for or accept the mobile number of a pupil/young person. There are no valid reasons why this should be necessary and to do so will create suspicion and place you in a vulnerable position.

- Don't have your mobile phone in view during lessons and never try to take photographs or videos of pupils/young people on your phone. If, as part of the learning experience, you need to photograph or video pupils/young people, get clear permission from the carer beforehand.

Social media

The proliferation of social media has blurred the boundaries of communication with its informality of approach. However, it's worth remembering for both teachers and pupils, certain rules should be adhered to in the interests of safety, security and privacy.

- You should not access your social media pages through any ICT equipment which does not belong to you.

- Your social media use including status updates or photo uploads should not identify or refer to them or refer to the pupils, young people, stakeholders, local authorities, carers or agency that you are working with.

- We would advise workers to refrain from engaging in, or commenting on topical news stories or discussions online that have a contentious nature within the education world – as it can result in complaints and concerns from parents, headteachers and Governors. In many cases, once your comments are published, you will not be able to have them removed. We suggest that you take a common sense approach, refraining from making any comments that could be perceived to be prejudicial, discriminatory or defamatory.

- We would also remind you that Facebook or other social media profile pictures can easily be accessed by pupils/young people; you should avoid using any photo which could be deemed inappropriate or suggestive. Monitor your privacy and security settings so that only friends can view your profile, otherwise pupils may be able to obtain your personal details.

- Finally, do not allow pupils to 'friend' you on Facebook (or any other social media) or make such a request yourself – even if you are coming to the end of your assignment. This will only blur the boundaries between pupil and tutor and will certainly put your motives in question.

- Do not share contact details with the pupil/young person