Online Tutoring Policy and Guidance

Introduction

Teaching Personnel takes its responsibility seriously for the safety of all those using online platforms to receive, deliver and track education, this can apply whether tutoring is carried out remotely, in school or as part of the National Tutoring Programme (NTP)Pupils, teachers/tutors, parents/carers, commissioning bodies and Teaching Personnel are all actively responsible for playing a role in ensuring online safety of both children and adults in the virtual/ remote learning environment, by taking measures to protect them from harm and keeping themselves safe in the broader setting of the virtual world. 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 Child and Vulnerable adult Protection policy.

Practices set within this policy must be followed to ensure safety. This applies to all individuals who access Company systems. It applies to information in all formats, including paper records and electronic data.

Remote working means working off the Company site. This includes working while connected to the Company's Wi-Fi networks.

A *mobile device* is defined as a portable device which can be used to store or process information. Examples include but are not limited to laptops, tablets, USB sticks, removable disc drives and smartphones.

Other relevant policies will include:

Child and Vulnerable adult Protection policy

Lone Working Policy

Procedures for Managing Allegations

Equal Opportunities and Diversity Policy

Child Protection Information

Data Protection Top Tips for Educators

Where relevant, the Teaching Personnel Educator should also be following the hirers policy and procedures relating to delivering virtual/ remote online learning.

Online Tutor

An online tutor is there to support and facilitate a learning experience and add extra value to the overall learning experience.

Online tutors support learners by:

- Responding to pupils' queries and providing their subject matter expertise
- Initiating learning activities for individuals or groups of pupils
- Providing feedback to tasks submitted, informally or as part of formal assessment
- Moderating and contributing to online discussions and live chat

All tutors are fully vetting in line with Teaching Personnel's vetting policy which exceeds the requirements of the DfE Keeping Children Safe in Education guidance.

Roles and Responsibilities:

It is the responsibility of the tutor to ensure that they work securely and protect both data and Company-owned equipment from loss, damage, or unauthorised access.

Tuition Managers are responsible for supporting tutor adherence with this policy. Additional measures may be put in place by management to ensure the rules contained within this policy are adhered to (for example monitoring or supervision).

Failure to comply with this policy may result in disciplinary action.

Key Principles of Video Conferencing

When using video conferencing facilities (For example Microsoft Teams, Zoom, Bramble, LEAP) as part of their day-to-day duties, Tutors must abide by the following: - Online Tutoring Policy and Guidance – Jan 2024

- 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 other to see.
- Avoid accessing video conferencing 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.
- Do not record calls without prior permission (see recordings below for details on when recording is necessary). In situations where recording is not necessary you may need to seek consent of users before recording. Please seek permission from Tuition Manager before doing so.
- 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 havea copy of data they may not be entitled to.*

- *Do not send chat logs: If you send the chat log at the end of a call to users, you could be sending data they are not entitled to see. Some chat logs include private messages on them so beware sending chatlogs to others.*

- 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 a sphone 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 provide with one by a school.

- If you want to implement new software to interact with pupils, please let your Tuition Manager know: We need to conduct a data protection impact assessment before using them. Whilst there are lots of creative ways to communicate and interact with others during these times, some of those technologies are relatively untested so we as a company need to consider any security risks to data .Please do ask your Tuition Manager in the first instance.
- Do report any behavioural or safeguarding concerns to your Tuition Manager 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.

Key Principles of Virtual Learning and Home Working

In addition to the principles above, it is important to comply with the following principles when conducting virtual learning and home working: -

- To adhere to the principles of the Data Protection Act 2018 and the Company's Data Protection Policy.
- Access to personal data must be controlled: For example, by locking office doors and locking computers.IT equipment used to process and store Company information in the home must be kept in a secure place where it cannot be easily accessed or stolen.

- Portable mobile devices should be encrypted where possible (or at least password/pin code protected) and should never be left unattended in a public place. IT equipment in the home used to process Company information should not be used where it can be overseen by unauthorised persons.
- It is the responsibility of each member of staff to ensure that they are working in a safe environment at home. No health and safety risks must be taken when using this equipment.
- All personal information and in particular sensitive personal information should be encrypted/password protected before being sent by email where possible. Extra care must be taken when sending emails where auto-complete features are enabled (as this can lead to sending emails to similar/incorrect email addresses).
- Always use your Company email address when contacting colleagues or pupils.
- Any technical problems (including, but not limited to, hardware failures and software errors) which may occur on the systems must be reported to your Tuition Manager immediately.
- Data should not be stored on personal devices. All data should be saved on Company systems.
- To be vigilant to phishing emails and not clicking on unsafe links. If clicked these links could lead to malware infection, loss of data or identity theft.
- Users should not access inappropriate websites on Company devices or whilst accessing Company networks. Users also must not do, cause, or permit any act or omission which will avoid coverage under the Company's insurance policy. If in any doubt as to whether particular acts or omissions will have this effect, the user should consult their Tuition Manager immediately.
- Users must only install software on Company equipment if authorised by the IT team. Please note that this includes screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

- Users who process Company data on their own equipment are responsible for the security of the data and the devices generally. In particular users should keep their device up to date with security software(such as anti-virus), report any loss or theft of device to your Tuition Manager.
- Any use of privately-owned devices by others (family or friends) must be controlled in such a way as to ensure that they do not have access to Company information. This will include Company emails, learning platforms and administrative systems.
- Using open (unsecured) wireless networks should be avoided. Consider configuring your device not to connect automatically to unknown networks.
- If the device needs to be repaired, ensure that the company used is subject to a contractual agreement which guarantees the secure handling of any data stored on the device.
- The Company may require access to a privately owned device when investigating policy breaches (for example to investigate cyber bullying).
- ll users must report any loss or suspected loss, or any unauthorised disclosure or suspected unauthorised disclosure, of equipment or data immediately to your Tuition Manager in order that appropriate steps may be taken quickly to protect Company data. Failure to do so immediately may seriously compromise Company security. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (whose email is **dataservices@judicium.com**).

The Tutor

The Tutor shall:

- Ensure that if no parent/responsible adult is present during a lesson session that the pupil is comfortable to continue the session; if not, they can terminate the session.

- Treat pupils fairly and without prejudice or discrimination; pupils who have a disability or come from a minority ethnic or cultural group can easily become victims of discrimination and prejudice which may be harmful to the pupil's wellbeing.
- Ensure that the tutor environment does not display any inappropriate images or documentation capable of being viewed by the pupil or parent/responsible adult when conducting a session.
- Ensure that sessions and contact with pupils only happen between the hours of 8:30 am and 4.30pm Monday to Friday (unless other special arrangements are made)
- Always ensure language is appropriate and not offensive or discriminatory.
- Ensure any contact with the pupil is appropriate to their role as a tutor and confined to the relevant lesson session.
- Not make any improper suggestions to a pupil.
- Not send personal or unsolicited communications via any means to the pupil or parent/responsible adult
- Value and take pupils' contributions seriously.
- Continue to look out for signs a child may be at risk and report and such concerns appropriately.
- Report any emergency, dispute or incident with a pupil or parent/responsible adult to Teaching Personnel in accordance with the Teaching Personnel Child and Vulnerable adult Protection policy.
- Report any inappropriate behaviour or illegal activity identified within a lesson session by the pupil or third party, in accordance with the Teaching Personnel Child and Vulnerable adult Protection policy.
- Follow the Key Principals of Video Conferencing contained within this policy

The Pupil

The pupil shall:

- Ensure that if no parent/responsible adult is present during a lesson session that they are comfortable to continue the session; if not, the session can be terminated.
- Ensure that sessions and contact with tutors only happens between the hours of 8:30 am and 4:30 pm Monday to Friday (unless other special arrangements are made)
- Treat the tutor with respect and fairness, and not subject them to abusive behaviour or language.
- Have no communication with the tutor outside the lesson session.
- Report any dispute or incident with a tutor to a parent/responsible adult as soon as possible.
- Report any inappropriate behaviour or illegal activity by a tutor within a session as soon as possible.

School/Parent/Responsible Adult

The school/parent/responsible Adult shall:

- Ensure the pupil is fully aware of the Teaching Personnel Child and Vulnerable adult Protection policy as well as the Safeguarding Policy of their school or the hirer.
- Ensure that if no parent/responsible adult is present during a lesson session that the pupil is comfortable to continue the session; if not, they can terminate the session.
- Ensure that sessions and contact with tutors only happens between the hours of 8:30 am and 4:30 pm Monday to Friday (unless other special arrangements are made)
- Always be responsible for the welfare of the pupil during the session.
- Continue to look out for signs a child may be at risk and report and such concerns appropriately.

- Always be responsible for the physical environment of the pupil during the session ensuring it is safe and appropriate.
- If they consider it appropriate, be present or available during a tutor session so any concerns encountered by the pupil can be reported as soon as possible and ensure the pupil and tutor are behaving in an appropriate manner.
- Ensure that tutors will be treated with respect and fairness by the pupil and will not be subjected to abusive behaviour or language.
- Ensure that no improper suggestions are made by either the tutor or pupil.
- Ensure the pupil has no inappropriate communication with the tutor outside the lesson session.
- Report any unsolicited communications between the tutor and pupil if appropriate
- Report any dispute in accordance with the Teaching Personnel Child and Vulnerable adult Protection policy.
- Report any inappropriate behaviour or illegal activity identified within a lesson session by the pupil or third party, in accordance with the Teaching Personnel Child and Vulnerable adult Protection policy.

National Tutoring Programme (NTP)

As part of their duties, Tutors will be expected to carry out tutoring in accordance with the National Tutoring Programme. Tutors will be provided with details of the NTP in order to effectively discharge their obligations.

In addition, there are specific guidelines which Tutors must follow when carrying out tutoring as part of the NTP scheme:

- 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.

- Tutor personal data will be collected by the Company for the purposes of tuition management and evaluation. This includes name, contact details, gender, region, occupation and qualifications and experience. Tutors will be provided a privacy notice detailing how their data is handled by the Company.
- Tutors will also have the opportunity to opt out of sharing data in this manner.
- Tutors must notify the Company immediately of a data breach. Any data breach under this scheme must be notified to the evaluators within 48 hours. Any unreasonable delay may result in further action being taken by the Company.
- Tutors should not have access to recordings.
- Should a school wish to use a different video conferencing platform to the Company default, the Tutor OR Tuition Manager will get the school to complete the video conferencing agreement to ensure recordings are available to the Company where necessary.
- Sessions will be recorded unless individuals have opted out to recordings. These will be managed internally by our Tuition Quality Assurance Manager. If a parent or pupil indicates they wish to opt out of recording, do let your Tuition Manager know immediately.
- From time to time, Tuition Managers 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.
- Pupil attendance and/or non-attendance must be recorded by tutors via our Virtual Learning Environment 'LEAP. This information is accessible to schools via the VLE platform.
- 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 your Tuition Manager.

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

Recordings

Company policy is that normal tutoring sessions should not be recorded unless agreement has been obtained by all parties. Tutors should seek approval of their Tuition Manager before recording any sessions. All sessions under the National Tutoring Programme are recorded due to regulatory requirements. Recordings must be saved on company systems and should not be transferred onto personal devices. This is to ensure this data is retained in accordance with Company retention guidelines. Recordings will be secured and disposed of safely in accordance with Company retention processes.

Further resources and guidance Keeping children safe in out of school settings:

Data Protection Top Tips for Educators

https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19 https://swgfl.org.uk/resources/safe-remote-learning/

https://coronavirus.lgfl.net/safeguarding

https://www.gov.uk/government/publications/education-for-a-connected-world

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf

https://www.saferrecruitmentconsortium.org

https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools/

Review: The Compliance Manager will keep this policy under annual review and/or if there have been any relevant legislative changes.