Tuke School On-line Policy

Our on-line policy reflects the need to reduce potential risks for students and staff. Recognising safety issues and planning accordingly will help to ensure that our students and staff are kept safe.

Curriculum Schemes of Work contain references to on-line safety where appropriate and teaching is modified to meet student needs, creating a safe learning environment.
We are aware of prioritising e-safety as our students are particularly vulnerable to e -safety risks. For example, our students may be vulnerable to cyber bullying, or they may not understand the concept of friendship and may trust everyone implicitly. This may affect their judgement about what to share in order to keep safe. We model appropriate behaviour when using e-devices in presentations for assemblies and in discussions with students and other staff.

We actively discourage use of personal devices connected to the school network; selected specific computers are used to scan devices prior to use in classrooms.
Tuke provides staff with 'clean' USB devices and encrypted USB devices if data is to be processed away from school. We have purchased services from RM which support antivirus software, firewalls and appropriate filtering.

Staff are aware that student data shared with them is of a confidential nature and that they do not share personal details between students/students and students/other adults.

Photography, videos and other creative arts
Whilst photographic and video images play a valuable role within the school curriculum, after-school activities and to celebrate achievement, staff should be aware that there is potential for such images and opportunities to be misused by adults with ulterior motives.

Staff should be sensitive to the needs of students who may have been abused in this way or who appear uncomfortable when asked to participate in photography or filming.

Staff should ensure that a member of the Leadership Team is aware of the proposed use of photographic/video equipment and that this is recorded in lesson plans.

Staff should be able to give account of the rationale behind any images of students that are in their possession. They should be stored securely and only used by those authorised to do so.

Permission from students and their parents/carers must be obtained for the use of images of students for publicity purposes and, in general, names of students will not be published.

Expected conduct in relation to the acceptable use of technologies and staff and student contact via social media.

Staff – The on-line policy is shared with all staff and forms part of the induction programme for staff. Contact between students and staff should always take place within clear and explicit professional boundaries, therefore, this section of the policy sets out the expectations to staff. It clearly identifies online activities that could breach the trust and confidence placed upon an employee and may constitute gross conduct: should read misconduct

- Staff should not access inappropriate materials using school computers or devices
- It is not permitted to 'friend' or 'follow' a student or parent on any social media platform. This also applies to ex-students.
- Any social media contact with students or parents should be via the school official social media account
- Staff should set the highest privacy settings on their personal social media accounts
- Staff should not respond to any friend requests from students, ex- students or parents on social media
- Staff should actively discourage ex- students taking photographs of them when making return to school visits.
- Staff should avoid posting any content on social media which may lead to questions about their personal or professional conduct. This may include making derogatory or insulting comments about sections of the community or individuals linked to school
- Staff should not post anything that is illegal or that can cause offence

Students are supported through Curriculum and Personalised Learning sessions to develop the skills to avoid harm and share concerns regarding use of computer and digital devices where appropriate.
Students can have a school email account where appropriate
Students who access online data or use school email should do so under supervision of staff at all times.
Students are supported to understand that they cannot carry their mobile phones around the school with them. Secure lockers are provided

Parents are provided with a copy of the on-line policy when their child starts at Tuke
Parents should not make requests for personal email accounts from staff
Parents should not make friend requests to staff using social media
Parents can use the office@tuke.southwark.sch.uk email to contact the school
We may invite parents to meetings regarding online safety as appropriate
Parents should discuss with the school any concerns they have in relation to online abuse targeted at their child

Resources to support this are found at http://www.thinkuknow.co.uk/teachers/resources/ using the SEN tab.
Share Aware – nspcc.org.uk
Parent Zone - CEOP

Communication and use of digital devices:

- All staff are supplied with an email account, currently hosted by RM and this is the preferred address to use for internal emailed communication.
- E mails are not considered private in the context of the school
- Emails containing reports sent out of school need to be encrypted
- Email contact to parents is always via the office email account office@tuke.southwark.sch.uk
- Student reports are shared using the school sever server and an email to confirm
- Staff only use school based accounts to communicate electronically with students.
- Instant messaging is not an accepted form of communication between staff and colleagues
- Staff cannot use their personal mobile telephone during work time, except in designated areas
- School mobile phones are to be used when off site

- Personal devices are not used to generate data unless the data is protected by a Tuke School password
- Data is not stored in portable devices overnight.
- All images are taken off from cameras and their flash memory chips within the same 24hrs.
- No images are stored in cameras overnight.
- Cameras used to record offsite activities are emptied before being taken out.
- No images of students are taken offsite
- Data regarding students is encrypted before being taken offsite
- We require any hardware, such as laptops, taken offsite, to be signed out.

Monitoring and implementing

All software downloads are managed by RM. Software downloads must in the first instance be requested from SLT before a request to RM for access is made. In the same way access to filtered websites must initially be requested from SLT before a request to RM is made to unblock access.

Staff should respond to and manage threatening or upsetting communications by informing senior leaders or governors at Tuke.
Tuke will seek advice and guidance from the Local Authority if necessary

The Head teacher reports on serious breaches of the policy to the Governing body.