SAND

Acceptable Use of ICT

Staff

October 2023

Use of Devices On Site

Under NO circumstances is an employee or customer of SAND authorised to engage in any illegal activity whilst on College site or on College WIFI whether college owned or a personal device.

The following activity is actively monitored and forbidden when own devices are connected to college Wifi or when own devices use own data but are on College sites or in College time.

Information which may lead to potential terrorism or extremist activity

Internet activity including sites categorised as:

- Intolerance
- Personal Weapons
- Terrorism
- Violence

Information which may lead to a potential risk to young people or vulnerable adults

Internet activity including sites categorised as:

- Adult Entertainers
- Adult Sites
- Child Abuse
- Pornography
- Restricted to Adults

Actively designed to harass, threaten, embarrass or target another person or group of people (cyberbullying)

Internet activity including:

- Online threats
- Mean, aggressive or rude tweets, posts or messages
- Posting of personal information, including pictures and videos

For security purposes SAND may monitor your network traffic at anytime. Your browsing history must be made available for the duration of internet use within College time, whether on SAND WIFI or your own data.

Staff Acceptable Use Policy

As a professional organisation with responsibility for safeguarding, it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the college's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list; all members of staff are reminded that IT use should be consistent with the college ethos, college policies, national/local guidance and expectations, and the Law.

1. I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

2. College owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will protect the devices in my care from unapproved access or theft.

4. I will respect system security and will not disclose any password or security information. I will use a 'strong' password to access college systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system.

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

6. I will ensure that any personal data of trainees, staff or parents/carers is kept in accordance with the Data Protection legislation (including GDPR).
    - This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.

- ○ Any data being removed from the college site (such as via email or on memory sticks or CDs) will be suitably protected. This may include data being encrypted by a method approved by the college.
- ○ Any images or videos of trainees will only be used as stated in the college image use policy and will always reflect parental consent.

7. I keep documents which contain college-related sensitive or personal information, including images, files, videos and emails, on designated devices only, and store information in a way that cannot be mixed up with personal data.

8. I will not store any personal information on the college computer system including any college laptop or similar device issued to members of staff that is unrelated to college activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the college's online safety policy which covers the requirements for use of mobile phones and personal devices and safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of learners within the classroom and other working spaces.

11. I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Designated Safeguarding Lead, Kate Wilson.

12. I will not attempt to bypass any filtering and/or security systems put in place by the college. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any college related documents or files, I will report this to the ICT Support Provider as soon as possible.

13. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using college or personal systems. This includes the use of email, text, social media, social networking, gaming and any other devices or websites.

14. I will promote online safety with the trainees in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

15. If I have any queries or questions regarding safe and professional practise online either in college or off site, I will raise them with the Designated Safeguarding Lead.

16. I understand that my use of the college information systems, including any devices provided by the college, including the college internet and college email, may be monitored and recorded to ensure the safety of young people and staff and to ensure policy compliance.

This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

17. I understand that the college may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance. Where it believes unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour may be taking place, the college may invoke its disciplinary procedures. If the college suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

Acceptance of payment from SAND confirms your acceptance of these terms.

Letter for Staff

Dear Employee

At The Sand Project we recognise that staff can be vulnerable to online risks. Social media can blur the definitions of personal and working lives; it is important that all members of staff at The Sand Project take precautions to protect themselves both professionally and personally online. We request that all members of staff:

- Are conscious of their own professional reputation and that of the college when online.
  - All members of staff are strongly advised in their own interests to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it.
  - Content shared online cannot be guaranteed to be "private" and could potentially be seen by unintended audiences. This could have consequences including civil, legal and disciplinary action being taken.

- Are aware that as professionals, we must ensure that the content we post online does not bring the college or our professional role into disrepute and does not undermine professional confidence in our abilities.
  - The teaching standards state that as professionals we should be achieving the highest possible standards in our conduct, act with honesty and integrity and forge positive professional relationships.

- All Staff be careful when publishing any information, personal contact details, video or images online.
  - It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Don't be afraid to be yourself online but do so respectfully.
  - Ensure that the privacy settings of the social media sites you use are set appropriately.
  - Consider if you would feel comfortable about a current or prospective employer, colleague, child in your care or their parent/carer, viewing or sharing your content. If the answer is no, consider if it should be posted online at all.

- Always use a work provided email address or phone number to contact trainees and parents – this is essential to protect yourself as well as the wider community.

- If you are concerned about a trainee's wellbeing or online behaviour, or if you are targeted online by a member of the community or are concerned about a colleague, please speak to the Designated Safeguarding Lead (Rachel McDonald-Taylor or Beki Tonks)
  - If you are unhappy with the response you receive then we request you follow our Whistleblowing procedure

Documents called “Cyberbullying: Supporting College Staff”, “Cyberbullying: advice for headteachers and college staff” and “Safer professional practise with technology” are available in below to help you consider how to protect yourself online.

- www.childnet.com/teachers-and-professionals/for-you-as-a-professional
- www.gov.uk/government/publications/preventing-and-tackling-bullying
- www.saferinternet.org.uk
- www.kscb.org.uk/guidance/online-safety

Additional advice and guidance for professionals is available locally through the Education Safeguarding Service or nationally through Professional Unions and/or the Professional Online Safety helpline www.saferinternet.org.uk/about/helpline

I would like to remind all staff of our Acceptable Use Policy and the importance of maintaining professional boundaries online. Failure to follow this guidance and the college behaviour policy could lead to disciplinary action; it is crucial that all staff understand how to protect themselves online.

Official Social Networking Acceptable Use Policy for Staff

1. As part of the college's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the college's approach to online safety. I am aware that X, Facebook and Instagram are public and global communications tool and that any content posted may reflect on the college, its reputation and services.

2. I will not use social media to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the college into disrepute.

3. I will not disclose information, make commitments or engage in activities on behalf of the college without authorisation. The MD retains the right to remove or approve content posted on behalf of the college.

4. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

5. I will follow the college's policy regarding confidentiality and data protection/use of images.
    - This means I will ensure that the college has written permission from parents/carers before using images or videos which include any members of the college community.
    - Any images of trainees will be taken on designated equipment, by the college and in accordance with the college image policy. Images which include trainees will only be uploaded by designated college staff via designated devices. Images taken for the sole purpose of inclusion on social media will not be forwarded to any other person or organisation.

6. I will promote online safety in the use of social media and will help to develop a responsible attitude to safety online and to the content that is accessed or created. I will ensure that the communication has been appropriately risk assessed and approved by the Designated Safeguarding Lead/MD prior to use.

7. I will set up a specific account/profile using a college provided email address to administrate social media accounts and I will use a strong password to secure the account. Personal social networking accounts or email addresses will not be used.

8. Where it believes unauthorised and/or inappropriate use of social media or unacceptable or inappropriate behaviour may be taking place, the college will exercise the right to ask for the content to be deleted or deactivated.

9. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

10. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the MD or DSL urgently.

11. I will ensure that social media is moderated on a regular basis as agreed with the college Designated Safeguarding Lead.

12. I have read and understood the college online safety policy which covers the requirements for safe IT use, including using appropriate devices and the use of social media.

13. If I have any queries or questions regarding safe and acceptable practise online, I will raise them with the MD or the DSL team

Acceptance of payment from SAND confirms your acceptance of these terms.