Policy name:	Acceptable Use Policy for Volunteers and Work Experience students
Author(s):	Lyssy Bolton
Date amended:	5 September 2023

Contents

Aims

- Protect children from the risk of radicalisation and extremism
- Protect systems and users from accidental or deliberate misuse that could put the security of the systems and users at risk
- Make users aware that internet use is monitored by the Trust for safeguarding purposes

Role of the Headteacher and Senior Leadership Team

The Headteacher and the Senior Leadership Team will:

- Ensure all volunteers are aware of and comply with this policy
- Provide guidance, support and training to all volunteers as necessary
- Monitor the effectiveness of this policy
- Display these guidelines around the school
- Keep a log of all ICT equipment issued to volunteers
- Provide training for all volunteers on induction and when the need arises
- Undertake risk assessments when required

Linked Policies

- Safeguarding and Child Protection

Acceptable Use Agreement

I understand that the school internet facility must be used only for educational purposes. I realise that I have a personal responsibility to abide by the set rules and regulations when using the internet and I am aware of the consequences if I breach them. This may include:

- Withdrawal of my volunteer / work experience placement
- Further monitoring of how I use the internet
- Disciplinary action
- Criminal prosecution

I will report immediately to the DSL / DDSL any accidental access to inappropriate material or websites.

In my capacity as a volunteer / work experience candidate I will:

- Immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the DSL / DDSL
- Communicate with others in a professional manner
- Only use social networking sites in school in accordance with the Trust's policies
- Check personal devices only during breaks and when not in the presence of children
- Use the network and cloud-based systems as directed to ensure that my data and documents are backed up and stored securely
- Always log on and fully log off devices to ensure that routine updates are carried out automatically
- Password protect any data that enables a third party to be identified when sending it outside of the local secure network
- Not send any data that enables a third party to be identified within the local secure network; sensitive information of this kind should be saved to an appropriate location and the recipient notified of that location
- Keep data private and confidential, unless it is essential to disclose such information for an appropriate purpose
- Ensure that all permission has been given to use the original work of others

I will not:

- Access, copy, remove or otherwise alter any other user's files, without their express permission
- Use the internet in such a way that it will bring the Trust into disrepute
- Use inappropriate or illegal websites
- Download inappropriate material or unapproved software
- Use inappropriate language
- Produce, send out, exhibit or publish material that will cause offence to anyone
- Divulge my login credentials or passwords to anyone
- Use the login credentials or passwords of any other user
- Use a computer that is logged on by another user
- Use any social networking site inappropriately
- Use personal email addresses for Trust business
- Use my personal equipment to record images / video

- Try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others
- Try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials
- Try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- Install or attempt to install programmes of any type on a machine, or store programmes on a computer without permission
- Contact children, parents / carers regarding school business (this should always be done by a member of staff, using the approved official school systems)

Signature:

- I understand that this policy applies to my placement and use of internet technology in school
- I understand that if I fail to comply with this policy, I could be subject to disciplinary action or Police involvement
- I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices within these guidelines