Acceptable User Policy

(Use of technology systems by staff)

Document Owner:	Brian Duffy
Approved By:	Helen Turner
First Publication Date	August 2020
Last Review Date:	August 2020
Audience:	All staff

Contents

Aims

This Acceptable Use Policy is intended as a 'code of conduct' for all SET employees, academy councillors, volunteers and external agencies when operating for SET. In addition, a 'pupil-friendly' version is worth producing by academies along the lines of this document. This policy is to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies
- that school ICT systems are protected from misuse
- that users are protected from potential risk in their use of ICT in their everyday work
- that staff are aware of good practice guidelines when using social networking as a member of our Academy

This Policy outlines guidance on use of internet and ICT facilities for work purposes for all staff and also gives advice and guidance on personal use of the internet, e.g. Social Networking sites, which will safeguard staff and ensure neither staff nor pupils are placed in vulnerable positions. The Policy covers 4 main aspects as follows:

1. Use of ICT Facilities within our academy
2. Use of Social Media/Networking sites by staff
3. Use of academy email system
4. Use of video conferencing platforms

It sits alongside, and should be read in conjunction with, all of our Safeguarding Policies, including our Online Safety Policy (e-safety), Online Monitoring and Filtering Policy, and of course our Safeguarding and Child Protection Policy. It also responds to the requirements of Keeping Children Safe in Education, which states, *"an effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate"*, and that schools should have a, *"staff behaviour policy which should…..acceptable use of technologies……and communications including the use of social media."*

In addition, the following SET policy/guidance documents should be referred to in conjunction with this policy:

- Data Protection Policy
- Data Security Policy

Introduction

The internet is a valuable resource to all schools and assists in raising educational standards by offering both pupils and staff opportunities to extend their knowledge and gain information from a very wide range of sources based throughout the world. However, the technology and the internet can also be 'misused' and it is important that clear guidance is given to both pupils and staff on appropriate use. It is important that staff understand that it is their responsibility to always act with the reputation of the Academy and Trust in mind and uphold professional standards at all time, including the use of technology and the internet, both within school and in personal time.

We, as an academy within The Shaw Education Trust respect privacy and understand that staff, academy council members, and volunteers may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy. Individuals are personally accountable for their behaviour when using digital technology and all individuals who work on The Shaw Education Trust premises, including agency, contract workers and volunteers are therefore required to support this policy.

Safeguarding children is a key responsibility of all members of staff and it is essential that all adults in our academy consider this and act responsibly if they are using internet sites either in or out of school. In addition, they must ensure that their own online behaviour protects not only the reputation of our academy, but also themselves against false allegations and misinterpretations which can arise from the use of internet sites.

Our academy operates its ICT systems for the benefit of our community and for the purposes of teaching, learning and research. All users of these facilities must abide by the regulations within this policy, placing reasonable limitations on behaviour and use to protect the school from misuse of its systems. ***All staff will be required to sign the Safeguarding Declaration Form at the start of each academic year and submit it to relevant colleagues within the academy. Staff will be prompted to do so each year.***

Use of ICT facilities within our academy

The use of ICT school systems brings with it a level of responsibility and professionalism that all staff must ensure they uphold. Systems must not be used in any manner that would in any way undermine the work or ethos of the school or any individual member of staff.

Users must not:

- Install new software without receiving approval from the relevant member of staff, e.g. Data Protection leads, System Managers and relevant line manager, especially any which may process personal or sensitive information of others. (This is to ensure all necessary licences are in place and that the software will not have an adverse effect on the network)
- View or transmit images, texts or other material that may be considered obscene indecent or abusive without authorisation
- Deliberately attempt to disable or change the network without authorisation
- Attempt to obtain unauthorised access to services and facilities of other Internet sites using school facilities
- Infringe someone else's copyright, e.g. by unauthorised copying or downloading of software
- Leave workstations unattended when logged on
- Use IT facilities and services for personal activities during work time
- Obtain material in any format that is illegal under the terms of any UK legislation (e.g. Race Relations Act, Obscene Publications Act, etc)
- Contravene any laws or regulatory requirements
- Share their passwords with others, including colleagues
- Allow parents, pupils, relatives or other unauthorised persons to see confidential information stored on the IMS
- Allow another person to log onto their IMS or to have access to confidential information. Where this occurs, it may be dealt with as a disciplinary matter
- Bring in viruses or malicious software
- Open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if there are concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

Users must:

- Keep their password secure. Your individual password must not be made available to anyone else except the System Managers, nor must the password be written down and displayed where others may see it
- Alert the relevant senior managers to any misuse of facilities

- Alert the Data Protection Officer where there is potential that the security of data may have been risked
- Alert the relevant senior managers to any health & safety issues
- When using mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school, follow the rules set out in this agreement, in the same way as if using school equipment. Ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- When transporting data and where digital personal data is transferred outside the secure local network, it must be encrypted. If this is not possible then this data should not be transferred outside the secure local network

Use of Social Media/Networking sites by staff

The purpose of this section is to outline the responsibilities for all employees when accessing social media technologies. It aims to manage organisational risk when using open social media technologies in both a personal and professional context and to enable employees to exercise good judgement in a digital world. It aims to support the E-Learning & IT Strategy in providing a safe and secure digital environment for our learners.

As an open organisation Shaw Education Trust recognises the value of social media as a powerful facility to engage and inspire the digital generation, and wider networking technologies is recognised as a key driver in the transformation of technology enabled learning if used in a responsible and professional way.

Social Media is a broad term for any kind of online platform which enables people to directly interact with each other. Examples of such sites include, but are not limited to blogs, Facebook, Twitter, YouTube, LinkedIn, Instagram, forums, bulletin boards, multiplayer online gaming, chatrooms, WhatsApp and instant messenger.

The 'dos' and 'don'ts' below apply to both use of social media:

Do's:

- Ensure adequate privacy settings are on all personal social media accounts and reviewed regularly
- Be aware of the potential of on-line identity fraud and to be cautious when giving out personal information about yourself which may compromise your personal safety and security

- Use social media sites in the teaching and learning process by all means. It is a good tool, but ensure use is appropriate to the work being covered and the age of pupils being taught (if ever in doubt staff should consult their line manager and/or Principal)
- Exercise good judgement at all times in line with all relevant SET policies, e.g. online safety policy
- Use social networking sites responsibly and ensure that neither personal/professional reputation, nor the academy's reputation is compromised by inappropriate postings
- Be professional, courteous and respectful as would be expected in any other situation
- Ensure communication between learners and adults takes place within clear and explicit professional boundaries
- Check with a Senior Leader before publishing content that may have controversial implications for the school
- Consider using a disclaimer when expressing personal views. Your personal views may not be representative of SET and may risk the reputation of the Trust

Don'ts:

- Do not 'befriend' any pupil at the school or under 18 unless already recognised as a 'family friend/acquaintance'
- It is also recommended not to befriend any student who has left the employees place of work within the last five years, even if over 18, unless considered a 'family friend/acquaintance'
- Staff are discouraged from identifying themselves as an employee of SET unless of course on an academy social media account. The line between public and private, professional and personal is not always clearly defined when using social media. If an employee identifies themselves as a member of staff of SET, this has the potential to create perceptions about the Trust to a range of external audiences and also among colleagues and pupils. Employees must be mindful of this when using social media
- Do not engage in any platform or discussions online which may bring the Trust into disrepute
- Do not breach any confidentiality by disclosing any work-related sensitive or privileged information
- Do not post or upload any inappropriate comments or images about colleagues, pupils, parents or businesses (including 'ex') associated with SET

- Do not access any illegal material
- Do not post material which may go against copyright law
- Do not post any image of a pupil on academy accounts unless permission has been given. This should never be done on personal accounts

Use of academy electronic communication systems

The importance of electronic communications is obvious to all and therefore it is advantageous to pupils to be able to use email systems to help their education and their progression of skills and experience in adult life. It is also important that all staff should have access to similar facilities to encourage planning of work through effective and appropriate communications. To protect staff and the school the following e-mail guidelines are used for good practice within our academy.

The guidelines below are suggested as a guide only to good practice for staff and can apply to ***all communications*** sent via an electronic network (e.g. email, bulletin board, on-line services, Intranet or Internet):

- Staff should not use full names of pupils when sending external emails/ unless deemed necessary for sharing information with other professionals
- Documents deemed to have confidential information should be sent with password protection facilities
- All communications should be treated as formal not informal. (Nothing should be included in an e-mail which would not be put into a traditional letter or memorandum)
- Check that messages are addressed to the intended recipient prior to sending, especially if the email is confidential/sensitive. *(To assist with workload, it is important to send to relevant staff and avoid global emails. It is the sender's responsibility to do so)*
- Staff should ensure they do not leave their email account open resulting in ability of others to access it
- Academy/Trust email accounts should be used for work purposes. (encryption methods should be encouraged when sending to external recipients)
- If staff accidentally access any unsuitable material, the site details must be reported to the Principal and/or network site manager
- When communicating with pupils via electronic systems, i.e. school email, staff must ensure that all the relevant points above are

applicable and ensure communications are professional at all times. Staff must cc in a colleague and if any safeguarding issues arise, report to their line manager and/or DSL asap using our normal academy safeguarding systems

NB. Academies can contact SET Data Lead colleagues to discuss practice around secure emailing processes.

In addition:

- Grammar and spellings should be checked, especially when being sent externally, as mistakes look just as unprofessional on screen as they do on paper
- Important to ensure that communications are factual and cannot be misconstrued
- Inserting relevant and detailed 'Subject' headings can ease management of emails

Use of video conferencing platforms

When any technology sees its popularity increase quickly, the number of things that can go wrong also increase. During the Covid-19 lockdown, meeting colleagues and other professionals online has become much more popular. But issues have arisen, e.g. issues initially with Zoom and reports of the app being 'hijacked'.

While hijacked meetings are disruptive and disturbing for participants, a more insidious threat is intruders who lurk in meetings without revealing their presence — a nightmare for security and individual privacy.

The good news is that many videoconferencing products include security settings that can prevent such incidents. The bad news is that it's often left to users with no security training to configure these settings.

Various platforms are in use and it is suggested that we use Microsoft Teams for internal communication, especially with smaller numbers. However, as it displays email addresses, it should not be used for any external conversations involving multiple people from different orgs as this could result in a data breach. Webex is useful for larger groups and external meetings. It is best to take advice from SET colleagues and Data Leads on video platform suitability before embarking on online communications.

The guidance below is to support staff and ensure protection for all, as much as possible, when using online platforms for video meetings. These can be used as guidance on any platform.

(Please note at the time of publication it is still Trust policy not to conduct live online teaching with any pupils except in identified schools with permission of CEO.)

Do use waiting room features in conferencing software. Such features put participants in a separate virtual room before the meeting and allow the host to admit only people who are supposed to be in the room.

Do make sure password protection is enabled. Make sure that your service uses both a meeting ID number and a password. If the service lets you create a password for the meeting, use password creation best practices — use a random string of numbers, letters, and symbols; don't create an easily guessable password like "123456".

Don't share links via social media posts. Invite attendees from within the conferencing software or via safe email systems — and tell them to not share the links, unless with colleagues.

Don't allow participants to screen share by default. Your software should offer settings that allow hosts to manage the screen sharing. Once a meeting has begun, the host can allow specific participants to share when appropriate.

Don't use video on a call if you don't need to. Turning off your webcam and listening in via audio prevents possible social engineering efforts to learn more about you through background objects. Audio-only also saves network bandwidth on an internet connection, improving the overall audio and visual quality of the meeting.

Do use the latest version of the software. Security vulnerabilities are likely to be exploited more often on older software versions. Double-check that participants are using the most upto-date version available.

Do lock a meeting once all the participants have joined the call if the facility allows this. However, if a valid participant drops out, be sure to unlock the meeting to let them back in and then re-lock it after they return.

Don't record meetings unless you need to. If you do record a meeting, make sure all participants know they are being recorded (the software should indicate this, but it's good practice to tell them too) and give the recording a unique name when you save it.

Do educate all staff who host meetings on the specific steps they should take in the software we use to ensure their conferences are secure.

Do not mention any individual pupil during the meeting nor share any information about a pupil, yourself or anyone else that may be traceable to an individual.

Do use background effects available on the platform or ensure your personal background does not display any information that is sensitive or could disclose any personal information about yourself or others or our Academy.

Do try to have someone whose job it is to 'manage the room' and focus just on doing that.

Do inform people what the Plan B is (i.e. if you do have to abort the meeting where will the meeting move to and how can people re-join).

Do turn off your video and microphone, unless it's needed.

For further information on a variety of online platforms staff should look online and always consult network manager or suitable individual for advice.

4 Potential and actual breaches of these regulations

Much of what is contained in this Policy is guidance on best practice, but it must be remembered that at all times the privacy and protection of individuals, our academy and our Trust are paramount. In instances where there has been a misuse of technology which puts at risk another member of staff, a pupil, the reputation of our Academy or our Trust due to a wilful act by a member of staff, it may be appropriate to implement the normal procedures of the relevant policies, i.e. our staff discipline policy. For more serious breaches it may be appropriate to involve the police, and as mentioned, where an incident puts the security of a pupils/staff/parent's data at potential risk, the Data Protection Lead should always be notified.

Statutory and other legal provisions allow for criminal prosecution of individuals accessing systems with the intention of causing damage or inconvenience (Computer Misuse Act 1990), for sending offensive, obscene or menacing messages (Telecommunications Act 1984), or for copying software without authority (Copyright Designs and Patents Act 1988).

Much of the information held on the network and databases are subject to the Data Protection Act 2018, General Data Protection Regulations and the Human Rights Act 1998 and as such are highly confidential. All staff that have access to systems must read and agree to comply with this protocol. Non-compliance could be a disciplinary matter.

Further Guidance

SET Data Protection Policy SET Data Security Policy	Guidance around the handling and sharing of information
UK Safer Internet Centre	Online safety tips, advice and resources to help children and young people stay safe online which includes relevant adult information.
UK Safer Internet Centre Social Media Guides	Information on the safety features available on these popular social networks.
UK Council for Child Internet Safety	Aimed at young people but examples of good practice included for all.
NEU Social Media and Online Safety	One professional association's guide to staff.
Ofsted's Guide to Inspecting e-safety	Report on Ofsted's inspection of online safety in schools

Below are website addresses to various video platforms. This is **not an endorsement** of these products by our academy nor the Shaw Education Trust but merely a link to the most commonly used platforms currently.

Microsoft Teams

Skype

Vimeo

Webex

Zoom (not recommended for use but an external organisation may use it if hosting a meeting with you)

Annex A: Staff Acceptable User Agreement Form

This form relates to the staff Acceptable Use Policy, available to all staff in our academy and across our Trust.

Please read the following statements. ***Staff will be asked each September to sign a declaration form which includes acceptance of this policy alongside some safeguarding aspects.***

All adults within our academy must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, email or social networking sites. They are asked to sign this agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must only use the school equipment, systems, e.g. email, social media etc. in an appropriate manner and for professional uses.
- I understand that I need to obtain/check permissions for children and young people before they can upload images to the internet.
- I know that images should not be inappropriate or reveal any personal information of children
- I have read the procedures details in the Acceptable Use Policy and SET's Social Media Policy
- I will report accidental misuse
- I will report any of concern for a pupil's safety to the DSL and/or the Principal. incidents
- I know that I am putting myself at risk of misinterpretation and allegation should I contact pupils via personal technologies, including my personal email. I know I should use the academy email address and telephones to contact parents
- I know that I must not use the academy's system for personal use unless this has been agreed by the Principal
- I know that I should complete virus checks on my laptop, memory sticks or any other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password, I will check with the

Principal or academy network manager prior to sharing this information

- I will adhere to copyright and intellectual property rights
- I will only install hardware and software I have been given permission for
- I accept that the use of any technology designed to avoid or bypass the academy's filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated
- Should I be a member of social networking sites, I will keep my profile secure and will avoid contact with parents, pupils and/or ex pupils related to our academy. I understand that any action or comment made by myself that brings our academy, our Trust or colleagues into disrepute or compromises pupil or staff confidentiality may be classed as a disciplinary matter

Shaw Education Trust

Shaw Education Trust Head Office,
Kidsgrove Secondary School,
Gloucester Road,
Kidsgrove,
ST7 4DL

Twitter @ShawEduTrust
LinkedIn @ShawEducationTrust
Call 01782 948259
Email info@shaw-education.org.uk
Visit shaw-education.org.uk

Pupil & people centred

Act with integrity

Be innovative

Be best in class

Be accountable