SWANLEA SCHOOL

Acceptable Use Policy for Staff

Acceptable Use Policy for staff, volunteers and visitors

Contents

1. Introduction

1.1 This Policy was researched and produced by the Associate Assistant Head for IT / Data and approved by the Head of IT services, Head Teacher, School Business Manager and Resources Governors.

1.2 The aims of this Acceptable Use Policy is to:

- Ensure that pupils benefit from all learning opportunities offered by the computing and internet resources provided by the school in a safe and controlled manner.
- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary policy / staff discipline policy/staff code of conduct].

2. GDPR - Data Security and Remote Access

2.1 Swanlea School holds a variety of sensitive data including personal information about students and staff as stated in our privacy notices. If you have been given access to this information, you are reminded of your responsibilities under General Data Protection Regulation (GDPR). You should only take a copy of data outside the school's systems if completely necessary. This includes having sensitive data onto laptops, USB memory sticks, iPads, external data plaforms such as sharepoint & Onedrive and emails. If you do need to take data outside the school, this should only be with the authorisation of the School Business Manager or lead Data Protection Officer. For good practice, you should perform a risk assessment on the implications of it falling into the wrong hands, and take appropriate steps to mitigate against this. This will almost certainly include encrypting the information, and checking the privacy notices of any recipients of the data. There are a variety of methods of remote access to systems available which allow you to work on data in-situ rather than taking it outside the school, and these should always be used in preference to taking data off-site. The IT Department at Swanlea offers a variety of information and support to help you keep data secure. If you are uncertain about any aspect of data security, you must contact them for or the School Business Manager for advice.

2.2 We comply with the following legislation and guidance:

Data Protection Act 2018

The General Data Protection Regulation

Computer Misuse Act 1990

Human Rights Act 1998

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Education Act 2011

Freedom of Information Act 2000

The Education and Inspections Act 2006

Keeping CHildren Safe in Educaiton 2022

2.3 Remote access & access to drives is available to all active employee user accounts at Swanlea School. The user log in credentials is to be used in order to get into the school's network. Assistance and guidance is provided by the IT Department if required. Remote connections are considered direct connections to the school network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy. All connection attempts are logged and can be viewed for monitoring purposes. When accessing any drives / remote access you must have set up second factor authentication which sends you a code to your personal device to verfify your identity.

2.4 **With regard to the equipment, the remote worker will be expected to:**

- Take reasonable care of the equipment.
- Take all reasonable steps to minimize the risk of theft or damage to
- School property and paperwork whilst these items are away from the school premises.
- Use it only for work purposes and in accordance with any operating instructions as defined in the Acceptable Use Policy.
- Comply with software licensing Terms and Conditions.
- Return to the school, the equipment at the end of the remote working arrangement

3. General

3.1 Virus protection and filtering software is used and updated regularly within the school network.

4. Pupils’ Access to the Internet

4.1 Swanlea School uses Webscreen filtering software run by LGFL, which will minimise the chances of pupils encountering undesirable material. We are using Sophos for our antivirus software.

4.2 Swanlea School will normally only allow pupils to use the internet when there is a member of staff present to supervise however an exception will be made for sixth form students.

4.3 Staff members are aware of the potential for misuse, and will be responsible for explaining to pupils the expectations the school has relating to responsible use of the internet.

5. Expectations of Staff, Volunteers, and Governors using the internet and school IT network

5.1 The school’s digital technology resources and systems will be used only for professional purposes or for uses as directed by the Head Teacher and Governing Body.

5.2 No data must be stored on external drives/sticks without permission from the Head Teacher and will only be given in exceptional circumstances.

5.3 Password(s) must not be revealed to anyone and will ensure this information is kept secret from all members of the school community.

5.4 Follow ‘good practice’ advice in the creation and use of your password. If your password is compromised, you must change it. Do not use anyone else’s password if they reveal it to you and advise them to change it. To change your password use this website https://support.lgfl.org.uk/

5.5 Do not share personal access details to e-mail/ Internet/ Intranet/ Network or other school systems, or any other / Local Authority (A) system with any other member of the school community – unless you are specifically requested to do so by the Head Teacher.

5.6 Any confidential/sensitive data printed and then no longer needed, needs to be placed in the confidential waste bin in the admin corridor.

5.7 Whilst in school, and out of school, do not use the school’s internet systems for any activity that may compromise your professional responsibilities or bring the school into disrepute.

5.8 Only use the school approved e-mail system(s) for school business, including communication with parents if not using the school text to parents system. Please note the school reserves the right to view any emails sent or received by any school representative.

5.9 Do not connect any personal device or software to the school’s network without approval from authorised personnel.

5.10 Do not use inappropriate or offensive language

5.11 Do not remove, delete, damage or dispose of ICT equipment, systems, programs, or information without permission form authorised personnel.

5.12 Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate will lead to disciplinary action

5.13 Gaining, or attempting to gain access to restricted area of the network, or to any password protected information, without approval from authorised personnel will lead to disciplinary action

5.14 Using the school's IT facilities to bully or harass someone else, or to promote unlawful discrimination will lead to disciplinary action

5.15 Only use the internet for professional purposes. Please be aware that all access to the internet is logged. Logs which reveal misuse of the internet which includes access to material which violates the Borough's Equality & Diversity policy and Prevent compliance may lead to disciplinary action.

5.16 Lock the screen when leaving your room or sign out.

5.17 Report any accidental access to, or receipt of inappropriate materials, or any filtering breach or equipment failure, to the ICT Technicians.

5.18 You are not authorised to download and install any software on the school network/ all requests for software must be made to the ICT Technicians and will be evaluated for appropriateness by the SLT line manager of the faculty. Do not make any attempts to alter or bypass the school's internet filtering systems or internet firewall systems.

5.19 Please check copyright and not publish or distribute any work, including images, music and videos, that is protected by copyright, without seeking the author's permission.

5.20 Communicate with others in a professional manner; do not use aggressive or inappropriate language and appreciate that others may have different opinions.

5.21 Be vigilant about attaching devices to the school network (e.g. USB or external drives) which may contain viruses and will not circumvent the anti-virus system if transfer of files is not allowed.

5.22 Social networking is only allowed in school on personal devices of members of staff in accordance with the e-safety policy and professional safe code of conduct policy.

5.23 Staff should not "become friends" or attempt to connect with current parents/carers or students (current and ex-students) on personal social networks for the protection of all concerned.

5.24 The data protection policy requires that any information seen by you with regard to staff or pupil information and held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that you are required by law to disclose such information to an appropriate authority.

5.25 Do not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted.

5.26 Do not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.

5.27 Only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure you only save photographs and videos of children and staff on the shared staff area (j: drive).

5.28 Use the school's Google Classroom platform in accordance with school protocols.

5.29 Only access school resources remotely (such as from home) using the school approved system and follow e-security protocols to interact with them.

5.30 Ensure any confidential data that you wish to transport from one location to another is protected by encryption, and that you follow school data protection guidelines.

5.31 You must never transfer personal data to an external organisation without the permission of the Headteacher.

5.32 Data protection policy requires that any information seen by you with regard to staff or pupil information that is held within the school's information management system will be kept private and confidential, EXCEPT when it is deemed necessary that you are required by law to disclose such information to an appropriate authority.

5.33 You must alert the school's child protection officer if you observe any behaviour by a member of the school community in connection with the school's IT systems which you feel is inappropriate and related to safeguarding.

5.34 Only use any other/LA system you have access to in accordance with its policies.

5.35 Report any damage or faults involving equipment or software immediately to the Building and Resources Manager or ICT Technicians.

5.36 You are not authorised, without permission, to create any blog/ social networking/ video / imagery etc. representing the school.This includes any representation of you as an employee of a school even if you do not explicitly say the schools name.

5.37 *Staff that have a teaching role only:* Ensure that you support the teaching and learning of e-safety/digital literacy as agreed with the development plan of your faculty.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher, or deputy headteachers will determine whether an act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

If you fail to comply with the Acceptable Use Policy Agreement, you could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/ or the Local Authority and in the event of illegal activities the involvement of the Police.

6. Sanctions

6.1 Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on disciplinary/professional staff code of conduct.

7. Use of photographs and/or video

7.1 Swanlea School uses photographs and/or videos to showcase our pupil's achievements and promote the school.

8. Staff (including governors, volunteers, and contractors)

8.1 The school's SBM and Network Manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the SBM.

9. Use of phones and email

9.1 The school provides each member of staff with an email address.

9.2 This email account should be used for work purposes only.

9.3 All work-related business should be conducted using the email address the school has provided.

9.4 Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

9.5 Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

9.6 Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

9.7 Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

9.8 If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

9.9 If staff send an email in error which contains the personal information of another person, they must inform the SBM immediately and follow our data breach procedure.

9.10 Staff must not give their personal phone numbers to parents or pupils. Staff must use phones/ softphones provided by the school to conduct all work-related business.

9.11 School phones/ softphones must not be used for personal matters.

9.12 Staff who are provided with mobile phones or softphone for their role must abide by the same rules for ICT acceptable use as set out in section 5.

10. Personal use

10.1.1 Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher or SBM may withdraw permission for it at any time or restrict access at their discretion.

10.1.2 Personal use is permitted provided that such use:

10.1.3 Does not take place during teaching or working hours

10.1.4 Does not constitute ‘unacceptable use’, as defined in section 5

10.1.5 Takes place when no pupils are present

10.1.6 Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

10.1.7 Staff may not use the school’s ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

10.1.8 Staff should be aware that use of the school’s ICT facilities for personal use may put personal communications within the scope of the school’s ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

10.1.9 Staff are also permitted to use their personal devices (such as mobile phones or tablets) in their own time and away from pupil areas.

10.1.10 Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

10.1.11 Staff should take care to follow the school’s guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

10.2 Personal social media accounts

10.2.1 Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

10.2.2 The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

10.3 School social media accounts

10.3.1 The school has an official Instagram and Twitter page, managed by the Media & Marketing Manager Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

10.3.2 The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

10.4 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity on the computers
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

11. Search and deletion

Under the Education Act 2011, and in line with the Department for Education’s guidance on searching, screening and confiscation, the school has the right to search pupils’ phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school’s rules.

12. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school’s ICT facilities should use safe computing practices at all times.

12.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action.

12.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

12.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

(see policies)

12.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the SBM

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the SBM immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

12.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Network Manager

13. Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by a member of SLT.

SLT will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

14. Monitoring and review

The headteacher, Head of IT services and SBM monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every two years.

The governing board is responsible for approving this policy.

15. Related policies

This policy should be read alongside the school's policies on:

- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Professional Safer Code of Conduct
- Data Protection

16. Definitions:

- **“ICT facilities”:** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **“Users”:** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **“Personal use”:** any use or activity not directly related to the users’ employment, study or purpose
- **“Authorised personnel”:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **“Materials”:** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

Appendix 1: Facebook cheat sheet for staff

Don’t accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don’t share anything publicly that you wouldn’t be just as happy showing your pupils
6. Don’t use social media sites during school hours
7. Don’t make comments about your job, your colleagues, our school or your pupils online – once it’s out there, it’s out there
8. Don’t associate yourself with the school on your profile (e.g. by setting it as your workplace, or by ‘checking in’ at a school event)
9. Don’t link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **‘Friends only’**, rather than ‘Friends of friends’. Otherwise, pupils and their families may still be able to read your posts, see things you’ve shared and look at your pictures if they’re friends with anybody on your contacts list
- Don’t forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you’ve **‘liked’**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can’t **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors

.

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and Head of IT services know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**