



SWANLEA SCHOOL
ACCEPTABLE USE POLICY
Students and Visitors

Comprehensive 2026 revision | Draft for formal approval

Document control	Details
Version	v2026.1 – comprehensive revision
Review date	23 September 2026
Status	Draft for approval by the Governing Body / LGB 01 Oct 26
Approved by	LGB 01.10.26
Policy owner	Head of IT Services / School Business Manager, with the Designated Safeguarding Lead (DSL) and Data Protection Officer (DPO)
Next review	September 2028, or earlier if law, DfE guidance, safeguarding risks, systems or practice change
Applies to	All pupils/students and visitors who use or seek to use Swanlea School ICT, networks, accounts, devices or digital services

Policy assurance note

This document updates the October 2024 student and visitor AUP using the structure and assurance approach of Swanlea School's 2026 comprehensive Staff AUP. It sets expectations and identifies evidence the school should retain. A written policy does not, by itself, certify that technical controls or local procedures are implemented; the school must verify its actual LGfL, filtering, monitoring, safeguarding, privacy and access arrangements before approval.



Contents

- 1. Purpose and scope
- 2. Legal, statutory and local framework
- 3. Roles and responsibilities
- 4. Core acceptable-use rules
- 5. Accounts, passwords and access
- 6. Devices, network and removable media
- 7. Filtering, monitoring and online safety
- 8. Cyber security and reporting incidents
- 9. Personal data and confidentiality
- 10. Learning platforms, email and communication
- 11. Loaned equipment and home use
- 12. Software and digital resources
- 13. Personal devices, photography and recording
- 14. Artificial intelligence and emerging technology
- 15. Visitors, contractors and parents/carers
- 16. Unacceptable use on and off site
- 17. Safeguarding, Prevent and reporting
- 18. Breaches, responses and sanctions
- 19. Training, review and assurance
- 20. Related policies
- 21. Compliance and implementation evidence
- Appendix A – Quick reporting guide
- Appendix B – Parent/carer agreement
- Appendix C – Younger pupil agreement
- Appendix D – Older pupil agreement
- Appendix E – Visitor acknowledgement
- Appendix F – Approval and implementation record



1. Purpose and scope

Swanlea School provides digital systems to support teaching, learning, communication and the safe operation of the school. This policy explains how pupils and visitors are expected to use those resources responsibly, lawfully and safely.

The aims are to:

- help pupils benefit from technology and online learning in a safe, supervised and purposeful way;
- set clear expectations for pupils, parents/carers, visitors and other authorised non-staff users;
- support safeguarding, online safety, data protection and cyber security;
- protect people, school information, equipment and services from misuse;
- explain how to raise concerns and what may happen when this policy is breached.

It applies on school premises and, where relevant, to activity outside school that affects the safety or wellbeing of pupils or the school community, involves school accounts or equipment, or is otherwise within the school's lawful remit. Visitors may use ICT only where access has been expressly authorised. A parent/carer does not automatically have access to the school network, staff systems or equipment.

Access is conditional on following this policy. The school may limit, suspend or withdraw access where necessary and proportionate to protect pupils, people, systems or information.

2. Legal, statutory and local framework

This policy is intended to be read alongside the current requirements and guidance applying in England, including:

- Keeping Children Safe in Education (KCSIE) 2026, including online safety and safeguarding responsibilities;
- Department for Education (DfE) digital and technology standards for schools and colleges, including filtering and monitoring and cyber security;
- Data Protection Act 2018 and UK GDPR, as amended where applicable by the Data (Use and Access) Act 2025;
- Computer Misuse Act 1990; Human Rights Act 1998; Equality Act 2010;
- Education Act 2011 and current DfE searching, screening and confiscation guidance, where applicable to pupils;
- Freedom of Information Act 2000, where relevant to school-held records;
- Copyright, Designs and Patents Act 1988;
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, where applicable to monitoring;
- LGfL safeguarding, online-safety and filtering resources;
- Tower Hamlets safeguarding, online-safety and Prevent procedures and resources currently applicable to the school.

The school should check the current versions and local requirements at each review. This list is a framework, not legal advice or a claim that every operational requirement is met.

3. Roles and responsibilities

Role	Responsibilities
------	------------------



Governing Body / authorised approver	Approves the policy and seeks assurance that safeguarding, filtering, monitoring and data-protection arrangements are reviewed.
Headteacher / senior leadership team (SLT)	Oversees implementation and proportionate responses to breaches, with safeguarding and operational leads.
Designated Safeguarding Lead (DSL) / deputy DSL	Leads safeguarding response, including online concerns and relevant filtering/monitoring alerts.
Head of IT Services / IT support	Maintains authorised access, technical controls, systems and incident response; supports checks and reviews.
Data Protection Officer (DPO) / School Business Manager (SBM)	Advises or coordinates data protection, privacy, breach, equipment and supplier matters under school procedures.
Teachers and supervising staff	Explain age-appropriate expectations, supervise use where required and promptly escalate concerns.
Students	Use systems for authorised learning, protect accounts and equipment, behave respectfully and report concerns.
Visitors, parents/carers and contractors	Use only explicitly authorised access, follow instructions, protect information and report concerns promptly.

4. Core acceptable-use rules

- Use school ICT for learning or another purpose expressly authorised by the school.
- Treat other people with respect online and offline. Do not bully, harass, threaten, discriminate against or impersonate anyone.
- Access only the systems, files, websites and information you are authorised to use.
- Keep passwords, passcodes and authentication information private. Never use another person's account.
- Protect personal, confidential and safeguarding information; do not browse, copy, photograph or share it without permission.
- Do not bypass or attempt to disable filtering, monitoring, security or device-management controls.
- Take care of school equipment and report damage, loss, theft or faults promptly.
- If unsure whether an action is allowed, stop and ask a teacher, supervising staff member or the relevant school contact.

5. Accounts, passwords and access

- Use only the account issued or approved for you, and only for its intended purpose.
- Never share your password or sign in for another person. Tell a teacher or IT immediately if you think someone knows your password or has used your account.
- Do not try to discover, guess, reset or obtain another user's password or authentication code.



- Do not attempt to access restricted network folders, staff systems, administrative tools or other people's files.
- Log out when finished and lock or close a device as instructed.
- If you can see information that appears to be private or outside your permissions, do not open, copy or share it; report it immediately.

6. Devices, network and removable media

- Use school devices and networks only as instructed and for authorised purposes. Treat all equipment carefully.
- Students and visitors must not connect USB storage, external drives or other removable media to school equipment unless a member of staff has specifically authorised it.
- Do not connect personal devices to the school network unless the school has expressly permitted it through an approved arrangement.
- Do not install applications, browser extensions, games, software or executable files, change settings, or connect unauthorised hardware.
- Do not use VPNs, proxies, custom DNS or other methods to evade filtering or access restrictions.
- Report damage, loss, theft, suspicious pop-ups or unexpected device behaviour to a member of staff promptly.

7. Filtering, monitoring and online safety

Swanlea's 2026 Staff AUP records use of LGfL WebScreen and Sophos. The school must confirm which services and configurations are currently active before publishing this policy.

Filtering is intended to prevent access to harmful or inappropriate content; monitoring helps identify activity that may require safeguarding, security or operational action. Depending on the service and configuration, school systems and school-managed devices may log or monitor internet requests, blocked sites, searches, account activity, device identifiers and use of school services.

- Filtering and monitoring must be configured for the school's risks and user groups, including pupils and guests where technically supported.
- Users must not assume that activity on school systems is private. Monitoring must nevertheless be lawful, necessary, proportionate, secure and explained through appropriate privacy information.
- If a website or resource is blocked but needed for learning, ask a teacher to use the school's approved review process. Do not try to bypass the block.
- If you encounter upsetting, sexual, violent, extremist, discriminatory or otherwise harmful content, stop viewing it and tell a teacher or the DSL. Do not forward it to others.
- The school should review filtering and monitoring at least annually and after significant incidents or material system changes, recording checks, findings and actions.

8. Cyber security and reporting incidents

Tell a teacher or IT immediately if you suspect a cyber incident, including phishing, malware, a compromised account, a lost device, unauthorised access or accidental disclosure.

- Do not open suspicious links or attachments or enter your password after following an unexpected prompt.
- Do not attempt to investigate, fix or delete evidence yourself. Follow staff instructions and preserve relevant information where safe.



- If you receive a message asking for passwords, personal information or money, do not respond; report it.
- Where a concern may involve personal data or a pupil's safety, staff should also escalate through the DPO/SBM or DSL route as appropriate.

9. Personal data and confidentiality

Personal information about pupils, families, staff or visitors must be treated with care.

- Do not access, copy, download, photograph, disclose or discuss personal or confidential information unless you are authorised and it is necessary for the approved purpose.
- Do not share another pupil's work, contact details, image, account information or personal circumstances without permission and a valid school-approved reason.
- Do not upload school or pupil information to personal email, personal cloud storage, messaging apps or public AI services.
- If information is sent to you by mistake, do not use or forward it; tell the sender and a member of staff.
- Report a suspected data breach immediately. Do not delete messages or files that may be relevant to an incident unless instructed by the person managing it.

10. Learning platforms, email and communication

10.1 Virtual learning environments

- Use Google Classroom and other school-approved learning platforms for learning and teacher-directed activities only.
- Upload only work and material requested or permitted by a teacher. Do not post offensive, unrelated, copyrighted, or personal material.
- Use class comments, chat, video and collaboration features respectfully and only for learning purposes.
- For remote lessons, follow teacher instructions about camera, microphone, chat, recording and attendance. Do not record, screenshot, livestream or share a lesson unless expressly authorised.

10.2 School email and messaging

- Use school-provided email for school learning and approved educational accounts. Do not use personal email to create accounts for school-directed platforms unless the school has expressly approved it.
- Communicate with teachers through the channels the school has provided. Do not use school systems for personal, abusive, threatening, or unrelated messages.
- Check recipients and attachments before sending. Do not open unexpected attachments or follow suspicious links.
- Do not impersonate another person, send messages from another account or circulate rumours, private information or harmful content.

11. Loaned equipment and home use

The school may loan equipment to support learning. The following conditions apply unless a written loan agreement sets additional or different requirements.



- Use the device for school-related purposes and follow the instructions supplied with it.
- Keep it secure, protect it from damage, and do not lend it to another person or allow others to use your school account.
- Do not install software, run unauthorised programs, remove management tools or alter security settings.
- Take the device only to locations authorised by the school. The 2024 arrangement specified the school and the pupil's home address; the school should confirm whether this remains current and record any approved exception.
- The school may manage, locate or monitor a loaned device where its configuration, privacy information and lawful purpose permit.
- Report loss, theft, damage or suspected compromise immediately. Return equipment when requested and follow the loan agreement's return deadline.
- Parents/carers are responsible for providing appropriate supervision at home and, where relevant, a safe internet environment. School filtering may not cover every home network or personal device.

12. Software and digital resources

- Use school-provided software only for the authorised educational purpose and in accordance with licence terms.
- Do not copy, share, redistribute, sell or install school-licensed software on other devices unless the licence and school expressly permit it.
- Respect copyright when using text, images, music, video and other online material. Credit sources as instructed.
- Do not download or distribute pirated material, unauthorised games or files, or content that is illegal or harmful.

13. Personal devices, photography and recording

- Personal devices may be used only in accordance with school rules, staff instructions and any applicable behaviour or mobile-phone policy.
- Do not use a personal phone, camera or other device to photograph, film, record or livestream pupils, staff, lessons or school activities without express authorisation.
- Do not upload or share images, audio, screenshots or recordings of another person without the necessary permission and school authorisation.
- Visitors must not photograph or record pupils or school areas unless permission has been given for the specific purpose. Follow any restrictions communicated on arrival.
- Where the school authorises photography or recording, use the approved equipment, consent process, storage and sharing arrangements.

14. Artificial intelligence and emerging technology

Students and visitors may use AI or other emerging tools only where the school has approved the tool and the activity. Teacher permission is required for pupil use in learning.

- Do not enter names, contact details, images, safeguarding information, school credentials, unpublished work or other personal/confidential information into public or unapproved AI tools.



- Do not use AI to impersonate, bully, harass, create sexualised images, produce threats, cheat or mislead others.
- Check and acknowledge AI assistance as directed by the teacher. Do not present generated work as entirely your own where this would breach school assessment rules.
- AI output may be wrong, biased or unsuitable. Follow teacher guidance and report harmful or concerning output.
- The school should assess age suitability, safeguarding, filtering, privacy, security and supplier terms before enabling learner-facing AI.

15. Visitors, contractors and parents/carers

- Visitors do not have automatic access to school ICT, Wi-Fi, accounts, devices or information. Any access must be explicitly approved and limited to the task.
- Use only the designated guest network or access method. Do not ask for or use a staff member's password or credentials.
- Do not access pupil records, staff systems, internal folders or confidential information unless specifically authorised for a legitimate purpose.
- Follow staff instructions about device use, photography, recording, supervision and access to school premises.
- Contractors and suppliers must follow the school's agreed confidentiality, safeguarding, security and data-processing requirements. Technical access must be authorised, limited and removed when no longer needed.
- Parents/carers should communicate respectfully through official school channels. Raise concerns or complaints directly with the school under its published procedures, rather than discussing identifiable pupils or staff in online groups.
- Do not post or share images of children other than your own unless you have the appropriate permission and the school's arrangements allow it.

16. Unacceptable use on and off site

The following are prohibited on school systems and may also be addressed when they occur outside school if they affect pupil safety, school operations or the school community, or involve school accounts/equipment:

- accessing, creating, storing or sharing illegal, pornographic, abusive, threatening, hateful or otherwise inappropriate material;
- cyberbullying, harassment, discrimination, intimidation, grooming, exploitation or impersonation;
- attempting to gain unauthorised access, bypass restrictions, interfere with systems or damage equipment;
- sharing passwords, confidential information, personal data or images without authority;
- copyright infringement, software piracy or unauthorised distribution of licensed resources;
- using ICT to promote unlawful activity, threaten others or bring harm to members of the school community;
- deliberately disrupting learning or school services, including spamming or knowingly introducing malware;
- using school ICT for commercial activity, gambling or unrelated activity without express permission.



This list gives examples and is not exhaustive. Context, age, safeguarding needs and the school's other policies will be considered.

17. Safeguarding, Prevent and reporting

Online safety is part of safeguarding. Students should tell a trusted member of staff if anything online makes them feel worried, pressured, unsafe, upset or threatened. Visitors should report concerns immediately to the DSL, deputy DSL or the staff member supervising them.

Report promptly any suspected grooming, sexual abuse or harassment, exploitation, threats, cyberbullying, self-harm or suicide-related concern, extremist/terrorist material or possible Prevent concern, or harmful contact involving a pupil.

- Listen calmly and take the concern seriously. Do not promise secrecy.
- Do not investigate, confront an alleged perpetrator, or ask a child to forward harmful images or messages.
- Record or pass on factual details through the school's safeguarding process. Do not circulate content.
- If someone is in immediate danger, contact emergency services through the appropriate route and alert school leadership as soon as possible.
- For allegations or concerns about an adult, follow the school's safeguarding procedure and relevant local arrangements, including LADO referral where applicable.

18. Breaches, responses and sanctions

A breach may lead to action under the school's Behaviour Policy, safeguarding procedures, visitor arrangements, loan agreement or other relevant procedure. The response will be proportionate to the nature, seriousness, impact, intent, age and circumstances of the incident.

- advice, teaching, restorative action or additional supervision;
- removal from a particular activity or restriction, suspension or withdrawal of ICT access;
- confiscation or search of a pupil's device only where permitted by current law and DfE guidance and in accordance with school procedure;
- parent/carer notification and a meeting where appropriate;
- recovery of reasonable costs for damage or loss where lawful and supported by the relevant agreement;
- ending a visitor's access or requiring them to leave the premises;
- referral to the DSL, DPO, local authority, police or another appropriate body where warranted.

The school will not treat this AUP as a blanket authority to search personal devices or access private accounts. Any search, inspection or evidence handling must follow the applicable law and school procedure. Immediate protective action may be taken where delay would create risk.

19. Training, review and assurance

- Pupils should receive age-appropriate online-safety teaching and reminders about reporting concerns.
- Visitors with approved ICT access should receive relevant instructions before access is provided.
- The school should retain evidence of AUP acceptance, visitor access authorisation, relevant training and incidents.



- Filtering and monitoring arrangements should be checked at least annually and after significant change, with findings and actions recorded.
- Review this policy at least annually, and sooner after a serious incident, material change in technology or guidance, or a change to school practice.
- The DSL, IT lead, DPO/SBM and leadership should contribute within their responsibilities; the Governing Body/authorised approver should approve the policy.

20. Related policies

- Safeguarding / Child Protection Policy
- Online Safety Policy
- Behaviour and Anti-Bullying Policy
- Mobile Phone / Personal Device Policy
- Data Protection Policy and Privacy Notices
- Cyber Incident and Data Breach Response Procedures
- Searching, Screening and Confiscation Procedure
- Visitor and Contractor Management Procedures
- Photography, Video and Image Consent Arrangements
- Prevent risk assessment and procedures
- AI / EdTech approval guidance
- Complaints Procedure
- Loaned Device Agreement

21. Compliance and implementation evidence

This matrix distinguishes policy wording from evidence needed to show the school's arrangements are operating. The school should complete the evidence column before treating the policy as implemented.

Area	Policy response	Local evidence to retain
KCSIE / safeguarding	Sections 3, 7, 17 and 19 set roles, reporting and review expectations.	Current safeguarding policy; named DSL/deputies and contact route; training and incident records.
LGfL / filtering and monitoring	Section 7 addresses user groups, blocked content, reporting and annual review.	Confirm active LGfL services; pupil/guest profiles; test results; alert ownership; annual review and action log.
Cyber security	Sections 5, 6 and 8 cover access, devices and incident reporting.	Current technical controls, guest access design, account review and incident response evidence.
Data protection	Section 9 limits access and sharing and requires prompt breach reporting.	Privacy information, relevant DPIAs, retention and breach procedures, approved systems list.
Tower Hamlets	Sections 2 and 17 refer to local safeguarding and Prevent	Check current borough procedures and record



	arrangements.	applicable referral/contact routes.
Visitors and contractors	Section 15 limits access and sets conduct expectations.	Visitor sign-in, access approval, induction/acknowledgement and contractor agreements.
Pupil agreements	Appendices B–D provide age-appropriate acceptance forms.	Signed/recorded acceptance and evidence of pupil explanation.

Local implementation checklist before approval

- ☐ Confirm current DSL/deputy DSL, IT and DPO/SBM contacts and reporting routes.
- ☐ Confirm whether LGfL WebScreen and Sophos remain the active services and document current configuration.
- ☐ Test and record filtering/monitoring arrangements for pupil and guest users where supported.
- ☐ Confirm visitor Wi-Fi, device and photography arrangements.
- ☐ Reconcile loaned-device location, recall and return conditions with current practice.
- ☐ Confirm approved learning platforms, AI tools and software; remove obsolete references.
- ☐ Check current Tower Hamlets safeguarding, online-safety and Prevent procedures.
- ☐ Confirm privacy information, monitoring transparency and any required DPIAs.
- ☐ Approve the policy and communicate it to pupils, parents/carers and relevant visitors.

Appendix A – Quick reporting guide

Concern	Tell	What to do now
Upsetting or harmful online content; pupil welfare concern	Teacher, DSL or deputy DSL	Stop viewing; do not forward; explain what happened.
Cyberbullying, threats, grooming, sexual content or exploitation	DSL/deputy DSL immediately	Preserve relevant details safely; do not investigate or circulate material.
Prevent / extremist concern	DSL or school Prevent lead	Report promptly; do not debate, repost or investigate yourself.
Phishing, malware, lost device or account compromise	IT / supervising staff immediately	Stop risky activity; do not delete evidence; follow instructions.
Personal information sent to the wrong person or exposed	Staff member, DPO/SBM via school route	Report immediately; do not forward or conceal the error.
Visitor access or conduct concern	Supervising staff/school leadership	Stop using the access and seek assistance.



Appendix B – Parent/carers acceptable use agreement

I have read and discussed this policy with my child, where appropriate. I will support safe, respectful and responsible use of school technology.

- I will use official school channels to raise concerns and communicate respectfully.
- I will not post identifiable information, allegations or images of other pupils or staff in online groups or social media.
- I will help my child keep passwords private and report concerns or suspected misuse.
- I understand that school ICT access may be restricted if the policy is breached.

Parent/carers name: _____ Child: _____

Signature: _____ Date: _____

Appendix C – Younger pupil agreement

When I use school computers, tablets or the internet, I will:

- use them when my teacher says it is okay;
- use them for my learning;
- keep my password secret;
- be kind and respectful online;
- not open things or visit websites my teacher has not allowed;
- tell a teacher straight away if something worries me or I see something I should not;
- look after school equipment and ask for help if something goes wrong.

Pupil name: _____ Class: _____ Date: _____

Parent/carers name and signature: _____

Appendix D – Older pupil agreement

I agree that I will:

- use school ICT, accounts and learning platforms only for authorised learning or activities;
- not access inappropriate sites, restricted files or another person's account;
- not share passwords, personal information or private images without permission;
- not bully, threaten, impersonate or harass anyone online;
- not install software, connect unauthorised storage or bypass filtering;
- follow teacher instructions for online lessons and never record or share them without permission;
- use AI only when allowed and never submit generated work dishonestly;
- report harmful content, safeguarding concerns, cyber incidents or mistakes promptly;
- understand that misuse may lead to action under school policy, including loss of access.

Pupil name: _____ Year/class: _____

Pupil signature: _____ Date: _____

Parent/carers agreement: I have discussed these expectations with my child and will support them in following this policy.

Parent/carers signature: _____ Date: _____

**Appendix E – Visitor acceptable use acknowledgement**

I understand that access to Swanlea School ICT is a privilege granted only for an authorised purpose.
I agree to:

- use only the account, network, device or information expressly authorised for me;
- not use or request staff credentials or access pupil/staff information without permission;
- protect any information I encounter and report accidental access or disclosure;
- not photograph, film or record pupils, staff or school activities without specific permission;
- follow school safeguarding, security and supervision instructions;
- report any safeguarding, cyber-security or data-protection concern immediately.

Name: _____ Organisation (if applicable):

Purpose / authorised access:

Signature: _____ Date:

Authorising staff member: _____ Access expiry (if applicable):

Appendix F – Approval and implementation record

Formal approval	Record
Approved by	_____
Role/committee	_____
Approval date	_____
Review date confirmed	_____

Control area	Owner	Date checked	Evidence/reference
Safeguarding contacts and local procedures			
LGfL filtering/monitoring review			
Guest network and visitor access			
Data protection / privacy information			
Pupil and parent agreement process			
Loaned equipment and approved EdTech			



External reference points for review

Check the live versions before approval and at each review:

- DfE – Keeping children safe in education: <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>
- DfE – Filtering and monitoring core standard: <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard>
- DfE – Cyber security core standard: <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-core-standard>
- DfE – Data protection in schools: <https://www.gov.uk/guidance/data-protection-in-schools>
- LGfL – Online Safety Audit: <https://lgfl.net/TypesOfHarm/OnlineSafetyAudit>
- Tower Hamlets – Safeguarding resources for schools:
https://www.towerhamlets.gov.uk/ignl/education_and_learning/schools/Safeguarding-resources-for-schools/Safeguarding-resources-for-schools.aspx