MAPLEWELL HALL SCHOOL

IT Acceptable Use Policy

Academic year 2026/27

Safe, secure, lawful and inclusive use of digital technology

Policy owner	IT Network Manager
Strategic accountability	Headteacher and Full Governing Body
Safeguarding oversight	Designated Safeguarding Lead
Approval date	Autumn 2026
Next review	Autumn 2027, or earlier if law, guidance, technology or school practice changes

Core rule
School technology must be used in ways that protect students, staff and the school; support learning and accessibility; respect privacy and confidentiality; and comply with safeguarding, data protection, equality and professional conduct requirements.

Contents

- 1. Policy statement and scope
- 2. Purpose and principles
- 3. Definitions
- 4. Legal and guidance framework
- 5. Roles and responsibilities
- 6. Access to school systems and accounts
- 7. Acceptable use
- 8. Unacceptable and prohibited use
- 9. Safeguarding and online safety
- 10. Filtering, monitoring and privacy
- 11. Data protection and confidentiality
- 12. Cyber security and technical security
- 13. Personal devices, communications and social media
- 14. Artificial intelligence
- 15. Incident reporting and response
- 16. Consequences and disciplinary procedures
- 17. SEND, accessibility and reasonable adjustments
- 18. Training and communication
- 19. Governance, approval and review
- 20. Related policies
- Appendix A. Staff Acceptable Use Agreement
- Appendix B. Student Acceptable Use Agreement - standard
- Appendix C. Student Acceptable Use Agreement - easy-read / symbol-ready
- Appendix D. Parent/Carer Home Learning and Device Loan Agreement
- Appendix E. Governor and Volunteer Acceptable Use Agreement
- Appendix F. Suggested login notice

1. Policy statement and scope

Maplewell Hall School is a maintained special school in Leicestershire for students aged 11 to 19. Digital technology is an essential part of teaching, learning, communication, safeguarding and school administration. This policy sets the whole-school framework for safe, secure, lawful, respectful and inclusive use of IT.

This policy applies to staff, students, governors, volunteers, supply and agency staff, contractors and other authorised users. It applies to school-owned or managed devices, accounts, networks, cloud services, software, communication platforms, storage and data, and to personal devices where they are used to access school systems or conduct school business.

The existing login notice may remain as a short point-of-access reminder. It does not replace this policy, the Staff Handbook, the Safeguarding and Child Protection Policy, the Artificial Intelligence Policy, or the relevant Acceptable Use Agreement.

SEND context
All students at Maplewell have an Education, Health and Care Plan (EHCP). Expectations must therefore be taught, supported and applied in ways that reflect age, developmental level, communication profile, cognition, sensory needs, vulnerability and individual support arrangements. A difficulty understanding or following a rule must not automatically be treated as deliberate misconduct.

2. Purpose and principles

The purpose of this policy is to:

- Protect students and adults from safeguarding, online, privacy, security and reputational harm.
- Set clear expectations for authorised use of school technology and information.
- Support learning, communication, independence, accessibility and preparation for adulthood.
- Protect personal, safeguarding, SEND, medical, personnel and other confidential information.
- Ensure filtering and monitoring are appropriate, proportionate, understood and reviewed.
- Provide clear routes for reporting and responding to incidents.
- Ensure consequences are fair, educational and proportionate, including reasonable adjustments where required.
- Support accountability through training, assurance, governing body oversight and annual review.

The school will apply the following principles:

- Safeguarding first: digital concerns are treated as safeguarding concerns where risk or harm may be present.
- Least necessary access: users receive access appropriate to their role, learning and level of supervision.
- Privacy and confidentiality: information is accessed, used and shared only where authorised and necessary.
- Security by default: passwords, devices, systems and data must be protected from loss, misuse and unauthorised access.
- Inclusion and accessibility: technology should reduce barriers and should not create avoidable new ones.
- Proportionality: monitoring, restrictions, investigation and consequences will reflect the nature and seriousness of the concern.
- Human responsibility: technology and automated tools do not replace professional judgement, safeguarding action or accountability.

3. Definitions

Term	Meaning
School IT / school systems	Devices, networks, internet access, email, cloud services, software, accounts, telephony, printers, storage, monitoring tools and other digital services provided, managed or approved by the school.
Authorised user	A person who has been given permission to use a school account, device, network or service.
Personal data	Information relating to an identified or identifiable person. Special category, safeguarding, health, SEND and social-care information require particular care.
Filtering	Technical controls that restrict access to inappropriate, harmful, unlawful or otherwise unsuitable online content.
Monitoring	Technical and/or human review of activity, alerts, logs or content for safeguarding, security, compliance, investigation, operational or service-management purposes.
Acceptable Use Agreement (AUA)	A role-appropriate agreement confirming that the user has understood and will follow the rules relevant to them.

4. Legal and guidance framework

This policy should be read in the context of current statutory duties and sector guidance reflected in Maplewell's existing policies, including:

- Keeping Children Safe in Education 2026.
- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
- Data (Use and Access) Act 2025.
- Equality Act 2010 and Human Rights Act 1998.
- Education Act 2002, section 175.
- Children Act 1989 and Children Act 2004.
- Children and Families Act 2014 and SEND Code of Practice: 0 to 25 years.
- Current Department for Education guidance and standards relating to online safety, filtering and monitoring, and digital technology in schools.

Where requirements are unclear or potentially conflicting, the school will seek advice from the Headteacher, Designated Safeguarding Lead (DSL), Data Protection Officer (DPO), IT Network Manager/network provider, local authority or legal advisers as appropriate.

5. Roles and responsibilities

Full Governing Body

- Approve this policy and review it at least annually, and sooner where significant changes occur.
- Ensure the school has appropriate strategic oversight of online safety, filtering and monitoring, data protection and cyber security.
- Receive proportionate assurance about implementation, incidents, training, accessibility and review, without unnecessary personal information.

Headteacher

- Provide strategic leadership and ensure this policy is implemented and understood.
- Ensure sufficient resources, training and leadership arrangements are in place.
- Make or delegate decisions on significant restrictions, investigations and disciplinary action in line with other school procedures.

Designated Safeguarding Lead

- Lead safeguarding responses to online or technology-related concerns.
- Work with IT staff and senior leaders on filtering and monitoring risks, alerts and emerging threats.
- Ensure safeguarding concerns are managed and recorded under the Safeguarding and Child Protection Policy.

IT Network Manager / network provider

- Manage accounts, permissions, devices, network access, security controls, filtering, monitoring, logging and technical incident response.
- Document the scope and limitations of technical controls and escalate safeguarding, security or data protection concerns promptly.
- Support the school's review of filtering and monitoring arrangements and maintain appropriate operational records.

Data Protection Officer

- Advise on data protection compliance, transparency, data sharing, breaches, retention, contracts and Data Protection Impact Assessments where required.
- Advise on the lawful and proportionate use of monitoring where personal data is processed.

All staff and authorised adults

- Use school systems professionally, lawfully and only for authorised purposes.
- Protect credentials and confidential information, follow professional conduct rules and report concerns promptly.
- Model safe, respectful and responsible digital behaviour.

Students

- Use technology for agreed learning and school purposes, following staff instructions and the student AUA.
- Keep passwords and personal information safe, treat others respectfully and report anything worrying, harmful or confusing.

Parents and carers

- Support safe use at home where school services or loan devices are used.
- Follow device-loan, security and reporting requirements and support students to understand the rules.

6. Access to school systems and accounts

- Accounts and devices are provided for authorised school purposes. Access may be limited by role, age, need, location, device type or risk.
- Users must use their own assigned account and must not share passwords, authentication codes or access tokens.
- Users must not attempt to access another person's account, files or communications unless formally authorised for a legitimate school purpose.

- Users must lock or log out of devices when leaving them unattended and must not deliberately leave authenticated sessions available to others.
- Administrative or elevated privileges may only be used by authorised personnel and only for legitimate duties.
- The school may temporarily suspend or restrict access where necessary to protect safeguarding, security, data or service continuity while a concern is assessed.

7. Acceptable use

Authorised users may use school IT to:

- Teach, learn, research and communicate for legitimate school purposes.
- Create, store and share school work using approved systems.
- Use approved accessibility and assistive technologies.
- Access approved online resources and services appropriate to the user's role and level of supervision.
- Communicate professionally through school-approved channels.
- Carry out administration, governance and operational duties within assigned permissions.
- Use approved AI tools in accordance with the Artificial Intelligence Policy.

Any incidental personal use by staff must be limited, lawful, appropriate, must not interfere with duties, create material cost or risk, or conflict with professional standards. The school may restrict such use where necessary.

8. Unacceptable and prohibited use

Users must not knowingly or deliberately:

- Access, create, store, send or share unlawful, abusive, discriminatory, threatening, exploitative, sexually inappropriate or otherwise harmful material.
- Use technology to bully, harass, intimidate, impersonate, deceive, humiliate or target another person.
- Attempt to bypass filtering, monitoring, authentication, device management, security controls or access restrictions.
- Install unapproved software, browser extensions, remote-access tools or applications where approval is required.
- Interfere with networks, devices, services or other users, including introducing malware or carrying out unauthorised security testing.
- Use another person's credentials or allow another person to use their own account.
- Access, alter, delete, disclose or copy data without authority.
- Use school resources for unlawful activity, personal commercial activity or financial gain unless expressly authorised for curriculum or school business.
- Infringe copyright, software licences or intellectual property rights.
- Use personal cloud storage or personal email for school information where school systems are provided and required.
- Record, photograph or film students on personal devices.
- Use unapproved AI services with identifiable student, safeguarding, health, SEND, personnel or other confidential information.

Accidental access
Accidental access to inappropriate content is not treated in the same way as deliberate access. The user should move away from the content where safe, avoid forwarding or sharing it, and report it promptly so that safeguarding or filtering action can be considered.

9. Safeguarding and online safety

Technology-related safeguarding concerns are managed under the Safeguarding and Child Protection Policy. This IT policy does not replace safeguarding procedures.

- Any concern that a student may be at risk of harm must be reported to the DSL or a deputy DSL without delay.
- Urgent concerns must be reported verbally; electronic recording must not delay immediate action.
- Staff must not investigate safeguarding concerns themselves, conduct repeated questioning or unnecessarily view, copy or forward harmful material.
- Online safety education will be age- and need-appropriate and will include privacy, respectful communication, harmful content, scams, misinformation, reporting and safe use of emerging technology.
- Where an incident involves child-on-child harm, staff will consider online contact, power imbalance, communication needs, SEND, vulnerability and ongoing risk.

Detailed safeguarding response, MyConcern recording, child-on-child abuse procedures, prohibited imagery procedures and allegations/low-level concerns routes are contained in the Safeguarding and Child Protection Policy and Staff Handbook and are not duplicated here.

10. Filtering, monitoring and privacy

The school will maintain filtering and monitoring arrangements appropriate to its students, network, devices and services. Technical controls support, but do not replace, supervision, education, professional curiosity and prompt reporting.

- Filtering and monitoring responsibilities will be allocated to appropriate senior leaders, the DSL, IT staff/network provider and governors.
- Arrangements will be reviewed at least annually and following significant incidents, system changes or emerging risks.
- Over-blocking, under-blocking, system limitations and accessibility impacts will be considered as part of review.
- Alerts or logs that indicate a safeguarding concern will be escalated through safeguarding procedures.
- Security or misuse alerts will be handled through the appropriate IT, management, data protection or disciplinary route.
- The school may record and review network, account, device and service activity where lawful and proportionate for safeguarding, security, compliance, investigation, service management or business continuity.

Monitoring disclosure for staff and other authorised adults
Activity on school-managed devices, networks, accounts and services may be logged or monitored. Users should not assume that school systems provide the same level of personal privacy as a private personal device or account. Monitoring must be proportionate, access-controlled and used only for legitimate school purposes. The school remains responsible for processing personal data lawfully, fairly, transparently and securely.

Product-specific filtering and monitoring arrangements are maintained in the school's safeguarding/online-safety documentation. They are not repeated in this policy so that operational controls can be updated without unnecessarily rewriting the whole policy.

11. Data protection and confidentiality

- Users must access only the personal information needed for their role or learning.
- Personal, safeguarding, SEND, medical, personnel and other confidential information must be stored and shared only through authorised systems and with authorised recipients.
- School information must not be copied to personal devices, personal email or personal cloud storage unless a specific authorised arrangement exists.

- Users must check recipients, attachments, sharing permissions and the minimum information necessary before sending or sharing data.
- Data breaches, loss, misdirection, unauthorised access or accidental disclosure must be reported immediately under the school's data-breach procedure.
- Records must be retained and deleted in line with the school's retention arrangements and applicable policy.
- Safeguarding information sharing follows the Safeguarding and Child Protection Policy; data protection law does not prevent necessary and proportionate safeguarding information sharing.

For detailed requirements on lawful processing, data subject rights, breach handling, privacy notices, retention and information sharing, refer to the Data Protection Policy and associated procedures.

12. Cyber security and technical security

- Use strong, unique passwords and multi-factor authentication where required.
- Do not disclose passwords or authentication codes to colleagues or other users, except through an approved technical recovery process.
- Do not disable school security controls, device management, filtering or monitoring.
- Do not connect unauthorised hardware, storage or network equipment to school systems.
- Report phishing, suspicious messages, unusual account behaviour, lost devices, malware warnings or suspected compromise promptly.
- Do not delete or alter potential evidence after a suspected security incident unless instructed by authorised IT staff.
- School-managed devices must be kept reasonably secure from theft, loss, damage and unauthorised use.

13. Personal devices, communications and social media

Detailed staff expectations for personal mobile phones, photography, communication with students and families, social media and professional boundaries are set out in the Staff Handbook. Those requirements apply alongside this policy.

- Staff must use school-approved communication routes for school business and must not use personal social media accounts to communicate with students.
- Personal devices must not be used to photograph, video or audio-record students.
- Students may use personal devices only where permitted by school rules, staff instruction and any individual plan.
- Any approved bring-your-own-device arrangement must use authorised access methods and must not weaken safeguarding, data protection or security controls.
- School data must not be stored on personal devices unless expressly authorised and appropriately secured.

14. Artificial intelligence

All AI use is governed by the school's Artificial Intelligence Policy. This IT policy therefore signposts, rather than duplicates, the detailed AI approval, privacy, assessment, bias, safeguarding and incident rules.

- Only approved AI tools may be used for approved school purposes.
- Identifiable or confidential information must not be entered into an unapproved AI service.
- AI must not replace safeguarding action, professional judgement or human accountability.
- Students must follow task-specific instructions and age restrictions and must not present AI-generated work as their own where this is prohibited.
- AI-related incidents must be reported through the appropriate safeguarding, data protection, IT, assessment or conduct route.

15. Incident reporting and response

Concerns must be reported according to their nature. A single incident may require more than one response route.

Concern	Immediate action	Primary route	Record / follow-up
Safeguarding / harmful content	Make safe; tell DSL/deputy without delay; do not investigate or forward harmful material.	DSL / Safeguarding and Child Protection Policy	MyConcern and safeguarding procedures.
Personal data breach	Stop further disclosure where possible; preserve relevant details; report immediately.	DPO / Data Protection Policy and breach procedure	Breach record and any required notifications.
Cyber security / suspected compromise	Contain where safe; report promptly; do not erase potential evidence.	IT Network Manager / network provider	Technical incident record and remediation.
Staff conduct / inappropriate use	Preserve relevant information; report through management or safeguarding route.	Headteacher / Chair / LADO as applicable	Conduct or safeguarding procedure.
Student misuse without safeguarding risk	Make safe; establish facts proportionately; restore learning and understanding.	Behaviour Policy / pastoral route	Behaviour or pastoral record where required.
Filtering / monitoring concern	Report over-blocking, under-blocking, inappropriate alerts or gaps.	IT Network Manager / DSL as appropriate	Operational review and safeguarding record if relevant.

16. Consequences and disciplinary procedures

Responses will be proportionate to the nature, seriousness, intent, impact and risk of the incident. The immediate priority is safety, safeguarding and restoration of secure systems.

16.1 Students

- Responses should normally be educational, restorative and linked to the school's Behaviour Policy.
- Staff will consider whether the student understood the rule, their communication and cognitive profile, impulsivity, vulnerability, previous teaching, level of supervision and any reasonable adjustments required.
- Possible responses include reteaching, additional supervision, a supported reflection, restricted access to a particular service or device, restorative work, family involvement, or other actions under the Behaviour Policy.
- Restrictions should be no broader or longer than necessary and should not remove access to essential learning or communication without an appropriate alternative.
- Where there is safeguarding risk, the Safeguarding and Child Protection Policy takes priority.

16.2 Staff and other adults

- Minor or inadvertent issues may be addressed through advice, retraining, management instruction or proportionate restriction of access.

- Repeated, deliberate or serious breaches may be managed under the Staff Handbook, code of conduct, capability, disciplinary, safeguarding, whistleblowing or other applicable procedure.
- Serious concerns may require referral to the LADO, police, regulator or other external body where appropriate.
- Technical access may be suspended temporarily where necessary to protect students, data, systems or an investigation.

17. SEND, accessibility and reasonable adjustments

Maplewell will not assume that the same wording, teaching method, level of independence or consequence is appropriate for every student.

- Provide accessible versions of rules using simplified language, visual prompts, symbols, photographs, social stories, modelling or other communication supports where appropriate.
- Teach acceptable use explicitly and revisit it regularly; do not rely on a one-off signature as evidence of understanding.
- Use communication methods suited to the student and allow processing time.
- Where appropriate, involve staff who know the student well while preserving the student's voice and dignity.
- Consider whether assistive technology or an adjustment changes how a rule should be applied, while maintaining safeguarding and security.
- Use proportionate consequences that take account of age, development, communication, cognition, disability, trauma, vulnerability and intent.
- Document individual adjustments or risk-management arrangements where they are significant or ongoing.
- Ensure accessible use does not create new barriers or expose students to avoidable privacy, safeguarding or security risk.

Accessible agreements
Appendices B and C provide a standard student agreement and an easy-read/symbol-ready version. Staff may produce an individual version using the student's usual communication system, provided the core expectations and safeguarding protections are retained.

18. Training and communication

The policy will be communicated in ways appropriate to each group.

Audience	How communicated	Minimum expectation	When
Staff	Induction, MyConcern/resources, email/briefing, relevant INSET.	Read policy and Staff AUA; confirm understanding; sign AUA annually.	On appointment and annually; updates when significant changes occur.
Students	Curriculum, online-safety teaching, tutor/pastoral work, individual support and accessible AUA.	Rules taught at an appropriate level; supported confirmation of understanding where meaningful.	At induction and revisited through the year.
Parents/carers	Website or parent communication, loan	Receive relevant expectations; sign device-	At issue of device and when material terms change.

Audience	How communicated	Minimum expectation	When
	documentation and home-learning guidance.	loan agreement where a device is issued.	
Governors	Policy papers, safeguarding/online-safety assurance and governor induction/training.	Read policy and relevant AUA; understand oversight responsibilities.	On appointment and at annual review.
Volunteers / contractors	Induction or briefing appropriate to access and role.	Agree to relevant acceptable-use, confidentiality and safeguarding requirements.	Before access is granted and when requirements change.

19. Governance, approval and review

- The policy will be approved by the Full Governing Body.
- It will be reviewed at least annually and sooner following a significant safeguarding, cyber-security or data-protection incident; a material change in law or guidance; a major technology or supplier change; an audit finding; or a significant change in school provision.
- The IT Network Manager will coordinate the operational review with input from the Headteacher, DSL, DPO, network provider and other relevant leaders.
- The Governing Body will receive proportionate assurance on implementation, filtering and monitoring, incidents, accessibility, training and actions arising from review.
- Changes affecting staff, students, families, governors or volunteers will be communicated through the routes in section 18.

20. Related policies

This policy should be read alongside the current versions of:

- Safeguarding and Child Protection Policy.
- Staff Handbook / Staff Code of Conduct.
- Artificial Intelligence Policy.
- Data Protection Policy and personal data breach procedure.
- Online Safety Policy, including filtering and monitoring arrangements.
- Behaviour Policy / Positive Behaviour for Learning arrangements.
- Equality and Diversity Policy and SEND-related procedures.
- Whistleblowing and allegations / low-level concerns procedures where applicable.

Where another policy contains the detailed procedure for a particular issue, that procedure applies. This IT policy sets the overarching acceptable-use framework and signposts users to the detailed route rather than duplicating it.

Appendix A. Staff Acceptable Use Agreement

This agreement applies to employees, supply staff and other adults using school IT in a staff capacity. It should be read with the IT Acceptable Use Policy, Staff Handbook, Safeguarding and Child Protection Policy, Artificial Intelligence Policy and Data Protection Policy.

Monitoring disclosure
I understand that use of school-managed devices, networks, accounts and services may be logged or monitored for legitimate safeguarding, security, compliance, investigation, operational or service-management purposes. I understand that school systems should not be treated as private personal systems, while the school remains responsible for lawful, fair, transparent and proportionate processing.

I will	I will not
Use my own account and keep passwords/authentication details secure.	Share credentials, use another person's account or leave an unlocked session available to others.
Use school-approved systems for communication with students and families.	Use personal email, personal social media or personal messaging to communicate with students.
Access only information I need for my role and keep it secure.	Store student or confidential information on personal devices, personal email or personal cloud storage unless specifically authorised.
Lock or log out of devices when I leave them unattended.	Attempt to bypass filtering, monitoring, authentication or device-management controls.
Use only approved software, services and AI tools for approved purposes.	Install unapproved software or enter identifiable/confidential information into an unapproved AI service.
Use school-owned devices for student photography, video or audio in line with school rules and consent arrangements.	Use a personal device to photograph, video or audio-record a student.
Report safeguarding concerns, data breaches, phishing, lost devices, suspicious activity and accidental access promptly.	Investigate safeguarding concerns myself, forward harmful material, or conceal an incident.
Follow copyright, licensing and professional conduct expectations.	Use school systems to bully, harass, discriminate, impersonate, deceive or access harmful/unlawful material.

I understand that failure to follow these requirements may lead to restriction of access, management action, retraining or action under the school's disciplinary, safeguarding or other relevant procedures, depending on the circumstances.

Name	
Role	
Signature	
Date	

Appendix B. Student Acceptable Use Agreement - standard

This version is for students who can understand the standard wording with normal staff support. Staff should adapt presentation, not weaken the core safeguarding and security rules.

I will	I will not
Use school devices and accounts for learning and other activities a member of staff allows.	Try to get around blocks, filters, monitoring or teacher instructions.
Keep my password private and ask for help if I think someone knows it.	Use someone else's account or tell other people my password.
Be kind and respectful when I use technology.	Use technology to bully, threaten, trick, embarrass or impersonate someone.
Tell a trusted adult if I see something worrying, upsetting, unsafe or confusing.	Share or forward harmful, frightening or inappropriate content.
Keep personal information about me and other people private.	Post, send or upload private information without permission.
Use approved AI tools only when a member of staff says I may.	Use AI to cheat, impersonate someone or put private information into an unapproved tool.
Look after school devices and tell staff if something is broken, lost or not working properly.	Deliberately damage devices, change settings I am not allowed to change, or install things without permission.
Follow staff instructions about cameras, recording and sharing images.	Take or share photographs, video or audio when I have not been given permission.

If I make a mistake

I will tell a member of staff. Staff will help me understand what happened and what I need to do next. The school will take account of my needs, understanding and circumstances when deciding what support or consequence is appropriate.

Student name	
Tutor group / class	
Student signature or supported confirmation	
Date	
Staff supporting understanding	
Parent/carer signature (where used)	

Appendix C. Student Acceptable Use Agreement - easy-read / symbol-ready

Use this version where simpler language is more appropriate. It can be presented with the student's usual school-approved symbols, photographs or communication system. Staff should teach each rule and check understanding rather than relying only on a signature.

✓ ASK I use the computer, tablet or internet when staff say it is OK.	**KEEP SAFE** I keep my password and private information safe. I ask an adult for help.
✓ BE KIND I use kind words. I do not use technology to hurt or upset people.	**STOP** If I see something that worries or upsets me, I stop and tell a trusted adult.
✓ USE MY ACCOUNT I use my own school account. I do not use someone else's account.	**✓ LOOK AFTER IT** I look after school devices. I tell staff if something is broken or lost.
✗ DO NOT BYPASS I do not try to get around blocks, filters or staff rules.	**✓ ASK ABOUT AI** I only use AI when staff say I can. I do not put private information into AI.
✓ ASK BEFORE PHOTOS I only take or share photos, video or sound when staff say it is OK.	

What happens if I get it wrong?
An adult will help me be safe and understand the rule. The school will think about what I understood, what support I need and what is fair for me.

Student name	
How the rules were explained / communication support used	
Student mark, signature or other agreed confirmation	
Date	
Staff member	

Appendix D. Parent/Carer Home Learning and Device Loan Agreement

Drafting note
The current Laptop Loan Agreement was not included with the documents supplied. This appendix therefore provides a policy-aligned draft and should be checked against the existing loan agreement before use, especially any clauses on damage, insurance, charging, accessories and return arrangements.

Where the school provides a device or access for home learning, the parent/carer agrees to support safe, secure and appropriate use.

Parent/carer commitments

- Support the student to use the device and school services for agreed educational purposes.
- Keep the device reasonably safe, dry and secure and use any protective case or accessories provided.
- Do not allow unauthorised people to use the student's school account or access confidential school information.
- Do not remove or interfere with school security, filtering, monitoring, device-management or access controls.
- Do not install software or make changes that the school has prohibited or that interfere with management of the device.
- Report loss, theft, damage, suspected compromise, inappropriate content or other concerns promptly to the school.
- Return the device, charger and supplied accessories when requested, when the student leaves the school, or when the loan ends.
- Support the student to follow the relevant student AUA, including rules about privacy, respectful behaviour, images and AI.

School commitments

- Provide reasonable guidance on safe use and the purpose of the loan.
- Apply school filtering/monitoring and device-management controls where technically available and appropriate.
- Explain how technical support and incident reporting can be accessed.
- Handle personal information collected through school systems in accordance with the school's data-protection arrangements.
- Consider accessibility and reasonable adjustments where required for the student.

Home internet and supervision
School technical controls reduce risk but do not remove the need for appropriate adult support at home. Filtering may work differently away from the school network depending on the device and service. Parents/carers should contact the school if they are unsure how a school-managed device behaves at home.

Student name	
Device / asset number (if used)	
Parent/carer name	
Parent/carer signature	

Date / school representative	

Appendix E. Governor and Volunteer Acceptable Use Agreement

This agreement applies to governors and volunteers who are given access to school systems, devices or confidential information. Access will be limited to what is needed for the role.

I will	I will not
Use school information only for my authorised governance or volunteer role.	Use confidential information for personal purposes or disclose it without authority.
Keep passwords, devices and documents secure.	Share credentials or allow other people to use my account.
Use approved school channels and systems where these are provided for my role.	Move school information to personal systems unless expressly authorised.
Respect safeguarding, confidentiality, equality and professional-boundary requirements.	Use technology to bully, harass, discriminate, impersonate or behave in a way that could place a student or adult at risk.
Report safeguarding, data-protection or security concerns promptly through the correct route.	Investigate safeguarding concerns myself or forward harmful material.
Use approved AI tools only for approved purposes and protect confidential information.	Enter identifiable, safeguarding, SEND, personnel or other confidential information into an unapproved AI service.
Understand that activity on school-managed systems may be logged or monitored proportionately.	Assume school-managed systems are private personal systems.
Name	
Role	
Signature	
Date	

Appendix F. Suggested login notice

The existing login notice can remain short. The following wording aligns it with the wider policy:

MAPLEWELL HALL SCHOOL - ACCEPTABLE USE NOTICE
Use this system only for authorised school purposes. Keep your password secure and do not use another person's account. Do not access or share harmful, unlawful or inappropriate material, bypass security/filtering/monitoring, or disclose confidential information without authority. Activity on school-managed systems may be logged or monitored for legitimate safeguarding, security, compliance and operational purposes. Report safeguarding, data-protection or security concerns promptly. By continuing, you agree to follow the school's IT Acceptable Use Policy and the rules that apply to your role.