Acceptable Use Policy
New Pastures Primary School

1	Summary	Acceptable Use Policy			
2	Responsible person	B Wray			
3	Accountable SLT member	B Wray			
4	Applies to	☒All staff ☐Support staff ☐Teaching staff			
5	Who has overseen development of this policy	SLT			
6	Who has been consulted and recommended policy for approval	Staff			
7	Approved by and date	September 2026			
8	Version number	Version 1			
9	Available on	Every	☐Y ☐N	Trust website Academy website SharePoint	☐Y ☐N ☒Y ☐N ☒Y ☐N
10	Related documents (if applicable)	• Online Safety Policy • Child Protection and Safeguarding Policy • Behaviour Policy • Data Protection Policy and privacy notices • Staff Code of Conduct and disciplinary procedures • Complaints Procedure			
11	Disseminated to	☐Trustees/governors ☒All staff ☐Support staff ☐Teaching staff			
12	Date of implementation (when shared)	September 2026			
13	Consulted with recognised trade unions	☐Y ☒N			

Purpose

Technology helps children learn, communicate and create. This policy sets clear expectations for safe, respectful and responsible use, protects personal information and explains what to do when something goes wrong. It works alongside the school's Online Safety Policy and safeguarding procedures.

In this document

Section	Page
1–3 Purpose, scope and responsibilities	2
4 Pupil expectations	3
5–7 Devices, home learning and AI	4
8–9 Filtering, monitoring and reporting	5
10–12 Adults, responses and implementation	6
Appendix A1 Parent and pupil form: EYFS/KS1	7
Appendix A2 Parent and pupil form: KS2	8

1. Purpose and principles

All users must use school technology lawfully, safely and for an authorised educational or professional purpose. The same expectations of kindness, respect and responsibility apply online and offline. The school will teach safe use, actively supervise pupils and respond to concerns promptly.

Children will be supported to report mistakes or worrying experiences. A child who asks for help or reports accidental exposure will be reassured. Safeguarding support will take priority where a child may be at risk.

2. Scope

This policy covers both school sites, school networks and internet services, computers, tablets, cameras and other digital equipment, school accounts, approved apps and communication platforms. It also applies to school devices and accounts used away from school, including remote learning.

Personal technology used in connection with school must follow the relevant school rules. Online behaviour outside school may be addressed where it affects pupils' safety, welfare or the school community, in line with the Behaviour Policy and safeguarding procedures.

This policy supplements the Online Safety Policy. Staff, governors, volunteers and visitors must also follow their existing acceptable use agreement, the Staff Code of Conduct where applicable, and Trust requirements. Appendix A1 or A2 is the combined parent/carer and pupil agreement for this policy.

3. Responsibilities

Who	Responsibilities
School/Trust governance	Approve the policy through the appropriate governance arrangements and receive assurance about safe technology use and effective controls.
Principal and DSL: Mr B Wray	Lead implementation, safeguarding decisions, online safety education and oversight of filtering and monitoring.
Deputy DSLs: Miss L Ward and Mrs C Cotton-Bailey	Receive concerns and support safeguarding action in accordance with school procedures.
Technical support: Alamo	Maintain authorised security and filtering arrangements, investigate technical faults and implement approved changes. Safeguarding decisions remain with the DSL.
Staff	Explain expectations, supervise pupils, model safe use, respond to concerns and ensure teaching and adjustments meet children's needs.
Pupils and parents/carers	Follow the relevant expectations, complete the appendix together and report concerns promptly.

Rules and agreements will be explained in accessible language, with adult support, translation, visual prompts or other reasonable adjustments where needed. Expectations and responses will take account of age, understanding and special educational needs and disabilities (SEND).

4. Pupil expectations

Use technology for learning

- Use school equipment, websites, apps and accounts only when an adult has allowed you to, and follow their instructions.
- Use only approved services. Games, messaging, social media and personal email must not be used unless specifically authorised for a learning activity.
- Do not download files, install software, make purchases, sign up to services or change settings without staff permission. Follow service age requirements; do not use a false age to create an account.

Be kind and respectful

- Communicate politely. Do not bully, threaten, deliberately exclude, humiliate or discriminate against another person online.
- Do not create or share harmful, offensive or sexual content, including altered images or AI-generated content. Do not impersonate another person.
- Ask staff before taking, recording, using or sharing images, video or audio. Respect other people's privacy and the school's permission arrangements.

Protect accounts and information

- Use only your assigned account, or a classroom account directed by staff. Keep your password private; ask a member of staff if you need help with it.
- Do not use someone else's account, open their files without permission, or share your account with another pupil.
- Do not share your address, telephone number, location, passwords or other personal information online. Ask an adult before entering information into a website or app.
- Do not open unexpected links, attachments, adverts or pop-ups. Tell an adult if an account, message or link looks suspicious.
- Log out when finished and follow instructions for shutting down or putting equipment away.

Keep school systems safe

- Do not try to reach blocked or unsuitable content, bypass filtering or monitoring, or use a proxy, VPN or personal hotspot to avoid school controls.
- Do not damage equipment, interfere with security settings or delete or change other people's work. Report damage, faults and mistakes straight away.
- Look after equipment, carry it safely and keep food and drinks away.

Think carefully and ask for help

- Check information rather than assuming it is true. Online information, images and AI answers can be wrong or misleading.
- Use your own work and acknowledge other people's work as your teacher explains. Do not copy material or present someone else's or AI-generated work as your own.
- Tell a trusted adult immediately about upsetting content, unkind messages, unexpected contact or anything that feels unsafe. Do not reply, forward it or investigate it yourself.

5. Personal devices and mobile phones

Under the school's Online Safety Policy, Year 5 and Year 6 pupils who walk to or from school may bring a phone when parental permission and school arrangements allow. It must be handed in or stored securely as directed. Pupils must not have access to it during the school day, including break and lunchtime, except for an explicitly authorised exception.

Other personal devices, including smart watches with messaging, recording or internet functions, must not be used without specific school approval. Personal devices must not be used to photograph, record or contact others, or to provide unfiltered internet access. An essential medical, disability-related or other agreed exception will be documented with suitable safeguards.

Parents should contact the school office if they need to pass an urgent message to their child. Misuse will be managed under the Behaviour Policy and may result in permission to bring a device being withdrawn. Searching or examining a device will follow current guidance and school procedures.

6. School devices and learning at home

- The same acceptable use rules apply to school accounts and devices away from school. Any equipment loan must follow its separate loan agreement.
- Use approved learning platforms and staff contact routes. Join live sessions only as instructed; do not share joining links or record sessions without school authorisation.
- Parents/carers should provide supervision appropriate to the child's age, understanding and activity, and tell the school if access or support is difficult.
- Keep equipment and accounts secure. Do not allow other people to use a child's school account, except where a parent/carer is supporting that child's learning as directed.
- Report loss, theft, damage, a compromised account or inappropriate content promptly. Do not attempt repairs or remove security controls.

School controls apply where technically configured and may not cover every device, app or home connection. The school will explain relevant arrangements and limitations when lending equipment. Families should not assume all home internet activity is filtered or monitored by school, or that monitoring provides an emergency response.

7. Artificial intelligence (AI) and new tools

Pupils may use an AI tool only as part of a staff-directed activity approved by the school. Staff must check suitability, age restrictions, safeguarding, privacy and the available controls before use. Approval of one tool does not authorise other tools or independent use.

- Do not put personal, confidential or safeguarding information, or identifiable pupil photographs, into an AI tool unless the school has specifically approved that use and its data protection safeguards.
- AI answers and images must be checked. They may be inaccurate, biased or unsuitable. Follow the teacher's instructions about acknowledging AI support.
- Do not use AI to impersonate someone, create humiliating or sexual images, or produce harmful content. Report a worrying response immediately.

8. Filtering, monitoring and privacy

The school uses Netsweeper for technical web filtering and monitoring. Filtering restricts access to harmful content; monitoring provides information or alerts about activity that may indicate risk. Neither replaces adult supervision, teaching or safeguarding judgement.

School devices, accounts, networks and internet activity may be logged and reviewed for safeguarding, security and proper operation of school systems. Authorised safeguarding, leadership and technical staff may access relevant records where necessary. Information is handled proportionately under the school/Trust's privacy notices, data protection policies and retention arrangements.

Netsweeper alerts are reviewed each school day by authorised leaders, with high-risk alerts considered as soon as practicable, as set out in the Online Safety Policy. Monitoring is not a guaranteed live or out-of-hours emergency service.

Users must report blocked legitimate learning resources, harmful material that is not blocked, suspected bypassing and technical faults. Only authorised staff may approve and implement changes. A user must not work around a block. The school formally reviews effectiveness at least annually and restricts affected internet use if safe controls are unavailable.

9. Reporting and responding to concerns

What pupils should do

Stop interacting and tell a trusted adult straight away. Do not reply to an unknown or harmful message, share it or continue looking for more information. Leave the device for an adult to manage. If the first adult is unavailable or the concern continues, tell another trusted adult.

What parents/carers should do

Contact the class teacher or school office promptly. Ask for Mr Wray, Miss Ward or Mrs Cotton-Bailey for a safeguarding concern. For non-urgent contact, email newpastures-admin@vennacademy.org. Emails may not be read immediately; speak to the school directly for an urgent school-day concern. If a child is in immediate danger, call 999.

Describe what happened, when, and the account or service involved. Do not email or forward sexual images of a child to the school. Ask the DSL how to handle any evidence safely.

What staff must do

- Ensure immediate safety; listen calmly, reassure the child and report a safeguarding concern immediately to the DSL or a deputy. Do not promise secrecy.
- Record safeguarding concerns on CPOMS in line with school procedures. Record behaviour incidents under the Behaviour Policy, including Stage 4 on Arbor where applicable.
- Report a lost device, compromised account, suspected data breach, filtering failure or security fault immediately through school/Trust arrangements and to technical support as appropriate.
- Preserve relevant evidence safely under DSL/technical direction. Do not conduct an unnecessary investigation or ask pupils to send harmful images.
- Do not view, copy, print, save or circulate a nude or semi-nude image of a child, including an AI-generated image. Refer the concern immediately to the DSL, who will follow the applicable safeguarding guidance.

10. Adults' acceptable use

Staff, governors, volunteers, visitors and other authorised adults must comply with the adult acceptable use agreement in the Online Safety Policy and their role-specific requirements. In particular, they must:

- Use approved accounts, devices and communication channels for school work; maintain professional boundaries and do not contact pupils through personal social media or private accounts.
- Keep credentials secure, use required security controls, lock unattended devices and prevent unauthorised access. Work devices and accounts must not be used by family members.
- Store and share personal or confidential information only through authorised school/Trust services. Do not copy it into personal email, storage or unapproved AI tools.
- Install software or change security settings only with authorisation. Respect copyright and report suspicious messages, faults and security incidents promptly.
- Use devices around pupils only for authorised professional purposes. Visitors and parents/carers must follow the school's no-mobile-phone-use-on-site arrangements unless specifically authorised.

11. Responses to misuse

The school will establish context before deciding a response. An alert or accidental access is not, by itself, proof of deliberate misuse. Responses will reflect the incident, risk, age, understanding, SEND and the needs of everyone affected.

Action may include additional teaching, pastoral support, restorative work, parental contact where safe, closer supervision, an appropriate Behaviour Policy consequence, or a proportionate restriction on an account or service. Essential learning and reasonable adjustments will be maintained through suitable arrangements. Adults' misuse may be addressed through professional conduct, disciplinary or visitor-access procedures.

Where there is risk of harm or suspected illegal activity, the DSL will follow safeguarding procedures and consider referral to children's social care, the police or other relevant agencies. Searches, confiscation and examination of data must follow current guidance and school procedures; this agreement does not provide blanket authority to search devices.

12. Agreements, implementation and review

Families complete either Appendix A1 (EYFS/KS1) or Appendix A2 (KS2), as appropriate to the child's understanding, on admission, annually and after a significant change. Staff explain and revisit the rules through computing, PSHE and everyday use. Signed forms are retained securely under school/Trust retention arrangements; families may request a copy.

A younger child may make a mark or have their understanding recorded by an adult. If a form is not returned or a family has concerns, school will discuss these and provide support; a missing signature alone will not remove access to the curriculum. The agreement acknowledges responsibilities. Separate permissions, including image/publication permissions, remain separate.

The Principal/DSL will review this policy annually, and sooner after a serious incident, significant technology change or change in guidance. It should be read with the Online Safety, Child Protection and Safeguarding, Behaviour, Data Protection and Complaints policies, privacy notices and Staff Code of Conduct.

Appendix A1. Parent and pupil agreement
EYFS and Key Stage 1

Complete one form per child. Choose the version that matches your child's age and understanding. Read it together, then return it to the class teacher.

Pupil name: _____

Class / year group: _____

My technology promises

1. I ask an adult before I use a computer, tablet or the internet.
2. I use the websites and apps my teacher says I can use.
3. I am kind when I use technology.
4. I keep my password and personal information private.
5. I ask an adult before I take or share a picture or recording.
6. I look after equipment and tell an adult if it is broken.
7. If something worries or upsets me, I stop and tell an adult straight away.
8. I finish and log out when my teacher tells me to.

An adult has talked about these promises with me. I will try to follow them and ask for help when I need it. Adults help check school technology to keep us safe.

Pupil signature or mark	Date

Parent/carer declaration

I have read the Acceptable Use Policy and discussed these rules with my child in a way they can understand. I will support safe use of school devices and accounts, appropriate supervision at home and the school's phone rules, and report concerns promptly.

I understand that school systems use filtering and monitoring, including Netsweeper, and relevant activity may be reviewed for safeguarding and security. These controls have limitations and are not an emergency service. I understand that misuse will receive a proportionate response under school policies.

This declaration acknowledges the rules; it is not consent for all data processing or for publication of my child's images. Separate permissions remain separate.

Parent/carer name: _____

Parent/carer signature	Date

Appendix A2. Parent and pupil agreement
Key Stage 2

Complete one form per child. Choose the version that matches your child's age and understanding. Read it together, then return it to the class teacher.

Pupil name: _____

Class / year group: _____

My agreement

1. I use school technology for learning, with permission, and follow staff instructions.
2. I use approved websites and apps. I do not install software, make purchases or sign up without permission.
3. I protect my password and personal information. I do not use someone else's account.
4. I am kind and respectful. I do not bully, threaten, impersonate or deliberately embarrass others.
5. I ask staff before taking, recording or sharing images, video or audio.
6. I do not bypass blocks or security controls, or open unknown links or attachments.
7. I tell a trusted adult immediately about upsetting content, unsafe messages, damage or mistakes. I do not forward harmful content.
8. I check information and credit other people's work. I use AI only when my teacher has approved and directed it.
9. If I bring a phone with permission, I hand it in or store it as directed and do not use it during the school day unless school has agreed an exception.
10. I follow these rules when using school accounts or devices at home, and log out when I finish.

I understand these rules and will ask for help if I am unsure. School systems are filtered and monitored, including through Netsweeper. Staff may talk to me about a concern, and misuse will receive a proportionate response.

Pupil signature or mark	Date

Parent/carer declaration

I have read the Acceptable Use Policy and discussed these rules with my child in a way they can understand. I will support safe use of school devices and accounts, appropriate supervision at home and the school's phone rules, and report concerns promptly.

I understand that school systems use filtering and monitoring, including Netsweeper, and relevant activity may be reviewed for safeguarding and security. These controls have limitations and are not an emergency service. I understand that misuse will receive a proportionate response under school policies.

This declaration acknowledges the rules; it is not consent for all data processing or for publication of my child's images. Separate permissions remain separate.

Parent/carer name: _____

Parent/carer signature	Date