NEW PASTURES

Information Technology Acceptable Use and Digital Safeguarding Policy Framework 2025-26

1.0 Institutional Context and Operational Parameters

1.1 This policy governs the use of information technology at New Pastures Care Farm.

1.2 The farm is located at Whitegates Farm, Chesterton Road, Harbury, Leamington Spa, CV33 9NH.

1.3 The farm is a specialist post-16 educational provision. It supports young adults with an Education, Health and Care Plan (EHCP).

1.4 Our students have complex needs. These primarily include Social, Emotional and Mental Health (SEMH) difficulties, autism, and emotionally based school avoidance.

1.5 Our ethos is to nurture achievement and celebrate success. The peaceful rural village setting provides a therapeutic learning environment.

1.6 We offer animal care courses, hair and beauty training, and social development services.

1.7 Technology must support learning without causing anxiety. It must not introduce new safeguarding risks.

1.8 This policy applies to everyone using our network. This includes staff, students, volunteers, and visiting professionals.

2.0 Statutory Foundations and Regulatory Compliance

2.1 The farm strictly follows national and local safeguarding laws.

2.2 We comply with the Department for Education's *Keeping Children Safe in Education* (KCSIE) guidance.

2.3 KCSIE mandates robust acceptable use policies. It also requires active internet filtering and monitoring systems.

2.4 The Designated Safeguarding Lead (DSL) oversees these monitoring systems.

2.5 We operate under the Warwickshire Safeguarding framework. Our policies align with local authority directives.

2.6 We routinely process highly sensitive EHCP data. Therefore, we strictly adhere to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2.7 We follow the Prevent duty to protect learners from online radicalisation and extremism.

3.0 Hardware Ecosystem and Environmental Risk Management

3.1 The farm provides Chromebooks for all students and staff.

3.2 We also maintain a segregated Windows computing environment. This is reserved for specialised administrative and vocational software.

3.3 Chromebooks are used because they boot quickly and have a simple interface. This reduces frustration and cognitive load for our students.

3.4 The IT administration centrally manages all Chromebooks. Users cannot install unauthorised software or browser extensions.

3.5 Whitegates Farm is an active agricultural environment. This poses severe risks to electronic devices.

3.6 Devices must be protected from hay dust, feed grains, water, and mud. These elements cause hardware failure.

3.7 Chromebooks must only be used in designated indoor educational or administrative spaces.

3.8 Devices must never be left unattended near livestock or used outdoors in bad weather.

3.9 Any damaged device must be surrendered to IT support immediately. Users must not attempt repairs themselves.

4.0 Cryptographic Security, Authentication, and Identity Management

4.1 Multi-Factor Authentication (MFA) is mandatory across the entire network.

4.2 All users must use a two-step verification process. This requires a password and a physical hardware security key (fob).

4.3 Physical hardware fobs offer the highest protection against phishing and cyber attacks.

4.4 Using a fob provides a physical anchor for authentication. This significantly reduces anxiety for students who struggle to remember complex rotating codes.

4.5 Passwords must be at least ten characters long. They must include a mix of letters, numbers, and symbols.

4.6 Passwords must not include obvious words. This includes the user's name, the farm's name, local Harbury identifiers, or animal names.

4.7 Hardware fobs can be easily lost on a farm. If a fob is lost, the user must report it immediately.

4.8 The administration will digitally revoke the lost fob to prevent unauthorised access. A temporary bypass code or a new fob will then be issued.

5.0 Network Utilisation, Acceptable Use, and Digital Boundaries

5.1 The IT network is strictly for educational, vocational, and administrative purposes.

5.2 Staff must only use institutionally provided email accounts for work.

5.3 Staff must never use personal email or personal social media to conduct farm business or contact students.

5.4 All users must communicate respectfully online. Harassment, discrimination, and defamatory language are strictly prohibited.

5.5 Users must not attempt to bypass web filters. The use of Virtual Private Networks (VPNs) or personal hotspots is forbidden.

5.6 Users must not modify hardware or attempt to introduce malware into the network.

5.7 Accessing, downloading, or sharing illegal, extreme, or sexually explicit content is a severe breach of policy.

5.8 Personal mobile phones are generally prohibited during educational hours. This reduces distraction and protects student privacy.

5.9 Recording audio, video, or taking photographs with personal devices is strictly banned everywhere on the farm.

6.0 Digital Safeguarding, Active Monitoring, and Threat Mitigation

6.1 Vulnerable learners face elevated risks online. We use an aggressive, multi-layered safeguarding approach.

6.2 The network automatically blocks access to malicious domains, adult content, gambling, and extremist sites.

6.3 Active monitoring software is installed on all devices. This software detects alarming search terms and keystrokes.

6.4 Alerts regarding self-harm, eating disorders, or violence are sent directly to the DSL.

6.5 The DSL reviews all alerts contextually. For example, animal care research may legitimately trigger alerts that would be suspicious elsewhere.

6.6 We enforce a zero-tolerance policy for cyberbullying and digital harassment.

6.7 Digital resilience is taught within the curriculum. Students learn about digital footprints, online consent, and how to report abuse.

7.0 Data Protection, Privacy, and Confidentiality Architecture

7.1 Staff must maintain absolute confidentiality regarding student EHCPs and safeguarding records.

7.2 Data access is strictly limited. Staff can only access the specific records required for their job.

7.3 Devices must be locked immediately when left unattended to prevent unauthorised viewing.

7.4 Sensitive data must only be shared via secure, encrypted channels.

7.5 Data must never be saved to unencrypted USB drives or personal cloud storage.

7.6 Capturing photos or videos of students requires explicit, documented consent.

7.7 Digital media must only be captured using farm-owned, encrypted devices.

7.8 Once captured, media must be moved to the secure internal cloud and deleted from the device immediately.

8.0 Accessibility, Cognitive Inclusion, and Comprehension

8.1 IT policies must be easily understood by all students.

8.2 The farm provides an Easy Read version of this policy. It uses simple words and visual symbols.

8.3 The Easy Read format strictly follows a "one idea per line" structure.

8.4 Staff must explain digital rules clearly and literally. They must avoid using confusing metaphors.

8.5 Chromebooks natively support essential accessibility features. These include screen readers, text-to-speech, and high-contrast displays.

8.6 IT staff regularly audit these tools to ensure they function properly and are not blocked by security updates.

9.0 Incident Response, Disciplinary Pathways, and Restorative Justice

9.1 Breaches of this policy are handled through a structured, restorative framework.

9.2 Tier 1 (Accidental): This includes forgotten passwords, lost fobs, or accidental hardware damage. The response focuses entirely on support and education. No disciplinary action is taken.

9.3 Tier 2 (Deliberate Misuse): This includes trying to bypass filters or sharing fobs. It results in a temporary suspension of network privileges and a restorative conversation.

9.4 Tier 3 (Severe Breach): This includes cyberbullying, accessing illegal content, or data theft. It results in immediate account lockdown, hardware confiscation, and statutory safeguarding referrals.

9.5 Staff must report any digital safeguarding concerns to the DSL immediately.

9.6 Students are provided with clear, safe pathways to report online abuse or mistakes without fear of immediate confrontation.

10.0 Strategic Policy Implementation and Review Mechanisms

10.1 This policy is a living document. It will be thoroughly reviewed on an annual basis.

10.2 Ad-hoc reviews will occur immediately following any cybersecurity incident or changes to national legislation.

10.3 The governing body of New Pastures Care Farm holds ultimate accountability for this policy.

10.4 Leadership will ensure that adequate resources and training are provided to maintain a safe digital environment.