IT, Internet and Online Safety Policy
Wayland Stables Care Farm

Policy owner and digital lead: Jake Payne, Business Manager

Online-safeguarding lead: Designated Safeguarding Lead (DSL) named in the current Safeguarding and Child Protection Policy

Approval date: 06/08/2026

Effective date: 01/09/2026

Next review: August 2027, or sooner after material change, incident or new guidance

Controlling status: On approval, this policy replaces the previous IT and Internet Safety Policy and Online Safety Policy. It operates with, and does not replace, the Safeguarding and Child Protection Policy, Data Protection Policy, Staff Code of Conduct and separate site-wide Mobile Phone, Smoking and Vaping Policy.

2026 transition: KCSIE 2025 remains in force until 31 August 2026. This policy incorporates the July 2026 information version of KCSIE 2026, which comes into force on 1 September 2026, and must be checked promptly against any final publication or correction.

1. Purpose, status and scope

Wayland Stables Care Farm (WSCF) provides non-school alternative learning and farm-based support for children and young people, including learners with special educational needs and disabilities (SEND), and supports adult participants. WSCF will provide a safe digital environment, teach safe and responsible use, protect information and systems, and respond promptly to online harm and cyber incidents.

This policy applies to business owners, employees, agency and temporary workers, volunteers, children, adult participants, parents and carers while using WSCF services, visitors, contractors, commissioners and third parties. It covers WSCF-owned or managed devices, networks, Wi-Fi, cloud services, email, messaging, websites, social media, cameras, audio/video, artificial-intelligence tools, removable media, remote access and any personal device authorised for WSCF work.

The DfE non-school alternative-provision national standards are voluntary as at August 2026 but are adopted by WSCF as its operating benchmark. KCSIE duties sit with the schools and colleges within its statutory scope; WSCF nevertheless adopts the relevant online-safeguarding controls as good practice and to support commissioners in meeting their duties.

1.1 Legal and guidance framework

- Children Acts 1989 and 2004, Education Act 2002 and Working Together to Safeguard Children 2026, as applicable to the parties involved;
- Keeping Children Safe in Education 2025 and the 2026 version effective from 1 September 2026;
- DfE statutory guidance on mobile phones in schools from 1 September 2026, applied by WSCF through its stricter whole-site rule;
- Counter-Terrorism and Security Act 2015 and Prevent duty guidance, where applicable to WSCF or the commissioning body;
- UK GDPR, Data Protection Act 2018 as amended (including by the Data (Use and Access) Act 2025), Privacy and Electronic Communications Regulations where relevant, and the Equality Act 2010;
- Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988, Protection from Harassment Act 1997, Sexual Offences Act 2003 and criminal communications legislation; and
- DfE filtering and monitoring and cyber-security standards, generative-AI guidance, UKCIS sharing-images guidance, ICO children's information guidance and NCSC advice.

2. Core principles and online risks

WSCF uses the four areas of online risk as a practical framework. A concern can sit in more than one category and can affect a child or adult participant even when it occurs away from the farm, on a private account or on a personally owned device.

Risk	Examples relevant to WSCF
Content	Pornography; extreme violence; self-harm or suicide material; racism, misogyny or misandry; antisemitism; radicalisation; misinformation, disinformation, conspiracy material and AI-generated or manipulated content.
Contact	Grooming; exploitation; adults posing as children; coercion; peer pressure; harmful interaction with other users; and AI applications or chatbots that simulate relationships or encourage dependency.

Risk	Examples relevant to WSCF
Conduct	Cyberbullying; harassment; hateful or sexual behaviour; making, requesting, sending or receiving nude or explicit images; deepfakes; doxxing; impersonation; non-consensual recording; and misuse of another person's account.
Commerce	Phishing, scams, fraud, gambling, loot boxes, inappropriate advertising, subscription traps, theft of credentials and pressure to buy or transfer money or digital assets.

- the best interests, voice, age, development, capacity and individual needs of the person;
- additional vulnerability associated with SEND, communication needs, trauma, care experience, mental ill health, social isolation or limited digital literacy;
- proportionate supervision, reasonable adjustments and the least intrusive effective control;
- privacy and data minimisation, without allowing confidentiality to delay necessary safeguarding sharing; and
- support and education as well as restriction: filtering is not a substitute for supervision, relationships, teaching or professional curiosity.

3. Governance, roles and responsibility boundary

Role	Responsibilities
Business Owners	Approve policy, resources and risk controls; oversee serious incidents and conflicts; obtain independent advice when required; and ensure commissioners receive assurance.
Jake Payne - Business Manager and digital lead	Lead implementation; coordinate IT support; approve systems and access; maintain asset, supplier, risk and incident records; commission annual reviews; and make sure leavers' access is removed promptly.
Victoria Addison - DSL, 07385 862158, victoria.addison@waylandstablescarefarm.co.uk	Lead online safeguarding; review alerts and incidents; support affected people; make or coordinate safeguarding referrals; and contribute to filtering, monitoring, AI and training reviews.
Shani Payne - Deputy DSL, 07758 247118	Provide safeguarding cover and act when the DSL is unavailable or the escalation route requires it.
Appointed internal or external IT support	Maintain secure configurations, filtering, monitoring, accounts, patches, backups and logs; investigate faults and incidents; provide reports; and explain limitations clearly.
Staff and volunteers	Use only authorised systems; model safe conduct; supervise learners; protect credentials and devices; report concerns immediately; preserve evidence; and complete required training.

Role	Responsibilities
Commissioning school or local authority	Retain its own placement, education and safeguarding duties; share relevant risk and support information; specify contractual controls; and act on incidents and review information reported by WSCF.
Children and adult participants	Receive accessible rules and support; use only approved devices, accounts and content; respect others; and report anything worrying, unsafe or suspicious.

A named person's absence or departure does not suspend a safeguarding, data or cyber-security duty. Jake Payne must record an interim responsible person and obtain competent external support where internal capacity or expertise is unavailable. A concern about Jake Payne must go to an uninvolved Business Owner and, where relevant, directly to the DSL, commissioner, local authority, police or regulator.

4. Site-wide personal-device and access rules

No-personal-phone site: Children, adult participants, staff, volunteers and visitors must keep personal phones, smartwatches, tablets, earbuds and other personal internet-connected or recording devices switched off and securely stored before entering WSCF-controlled learning and activity areas. The separate Mobile Phone, Smoking and Vaping Policy controls storage, exceptions and breaches.

- Children and adult participants must not access a personal device during a session. Staff must never give a participant access to a staff member's personal device.
- A documented exception may be approved for a disability, medical need, safeguarding plan, emergency, multi-factor authentication or essential operational task. It must specify the person, device, purpose, location, supervision and end point.
- Staff should use the WSCF radio system for routine site coordination. An authorised work phone must be used discreetly, away from participants where practicable, and never while supervising a hazardous activity.
- Personal hotspots, portable Wi-Fi, VPNs, proxies, private DNS, tethering or other methods that bypass WSCF controls are prohibited unless specifically approved and technically managed.
- Guests and unmanaged authorised devices must use the designated guest or segregated network. Access credentials must not be displayed publicly or shared beyond the intended user group.
- WSCF may withdraw network or device access immediately where necessary for safety, security or investigation. Any search, confiscation or disciplinary response involving a child remains the responsibility of the commissioning school unless a

lawful agreement says otherwise; WSCF will secure the immediate situation and report it promptly.

5. Acceptable use of systems and internet

5.1 Required conduct

- Use WSCF systems only for authorised learning, care, administration or operational purposes and only within the access granted to the user.
- Use an individual account where one is provided; keep passwords, passkeys, security keys and codes confidential; lock the screen when leaving a device; and sign out after use.
- Use approved WSCF email, storage, communication, learning and recording systems. Do not move work to a personal email account, personal cloud drive, personal messaging service or unapproved app.
- Respect copyright, licences, confidentiality, privacy and the rights and dignity of other people.
- Check the intended recipient, attachment, link and sensitivity before sending or sharing information. Use approved secure-transfer methods for confidential or safeguarding material.
- Report unexpected content, blocked searches, suspicious messages, phishing, compromised credentials, lost devices, unauthorised access, bullying, grooming, sexual material, scams or any other concern immediately.

5.2 Prohibited use

- accessing, creating, requesting, storing or sharing illegal, sexual, abusive, hateful, violent, extremist or otherwise harmful material except where an authorised professional task has been risk assessed and approved;
- bullying, harassment, discrimination, threats, sexualised conduct, impersonation, doxxing, grooming, exploitation, coercion or encouraging self-harm;
- attempting to disable, evade, probe or bypass filtering, monitoring, security, licensing, permissions, audit logs or device-management controls;
- installing software, browser extensions or removable media, connecting equipment, changing security settings or creating accounts without authorisation;
- using another person’s account, sharing credentials, leaving a logged-in device for another person, or seeking access beyond the user’s role;

- cryptocurrency mining, unauthorised commercial activity, gambling, fraud, scams, mass messaging or activity likely to disrupt systems; and
- photographing, filming, recording, live-streaming or publishing information about any child or adult participant without the specific authorised process.

6. Staff conduct, communications and social media

- Staff and volunteers must maintain the same professional boundaries online as in person and comply with the Staff Code of Conduct and safeguarding procedures.
- Do not friend, follow, privately message, game with or communicate through a personal account with a child or participant. Use only an approved channel, for an authorised purpose, with appropriate oversight and records.
- Do not share personal contact details, location, private life information or access to personal profiles with participants. Review privacy settings but never rely on them to make inappropriate contact acceptable.
- Do not post or discuss confidential WSCF business, incidents, colleagues, children, adult participants, families or commissioners on personal social media, even where names are omitted.
- Do not use disappearing-message functions for WSCF work. Necessary communication must be capable of being retained and retrieved through an approved system.
- A safeguarding concern about an adult's online conduct, including boundary breaches, must be reported through the concerns/allegations route in the Safeguarding and Child Protection Policy; it must not be investigated informally by colleagues.

7. Learning, supervision and digital resilience

Internet access by children or adult participants must be purposeful, planned, risk assessed and supervised at a level matched to age, development, capacity, SEND and known vulnerabilities. WSCF-owned or specifically approved devices and accounts must be used. Staff must know the learning objective, content or service, account arrangement, filtering coverage and action to take if something unexpected appears.

- teach or reinforce how to recognise the 4Cs, manage privacy, verify information, identify AI-generated or manipulated material, resist scams and coercion, seek help and support peers safely;
- use accessible language, visuals, repetition, modelling and supported practice; avoid fear-based or blame-based teaching;

- explain in age- and ability-appropriate terms that activity on WSCF systems may be filtered and monitored and how concerns are handled;
- give participants a safe way to report privately and make clear that accidental exposure or asking for help will not in itself lead to blame;
- prepare for sensitive topics, identify support and safeguarding routes, and avoid searching for illegal or graphic examples; and
- share proportionate information with parents, carers and commissioners about planned online activity, systems used and material incidents, subject to safeguarding and confidentiality decisions.

8. Filtering and monitoring

Where WSCF controls a network, account or device used by children, it will apply filtering and monitoring proportionate to the user profile and risk. No system is fully effective. Technical controls must operate with active supervision, education, professional curiosity and an immediate reporting route.

- Jake Payne, the DSL and IT support will complete and record a formal review at least once every academic year and after a significant incident, safeguarding change, new device or service, generative-AI introduction, major update, remote-access change or evidence that controls are ineffective.
- The review will cover all internet connections, WSCF-managed devices including those used off site, authorised unmanaged devices, guest access, apps, image/audio/video and dynamic or AI-generated content, different user profiles and all relevant site locations.
- Checks must establish that illegal child sexual abuse material, unlawful terrorist content and adult content are blocked as a minimum; that required IWF and CTIRU blocklists are maintained by the provider; and that bypass tools and backup connections are addressed.
- WSCF will maintain separate, appropriate access profiles for learners, staff and guests. Over-blocking must not unreasonably prevent learning or the teaching of online safety.
- The check log must record date, person, device/location/profile tested, what was checked, result, limitation, action owner and completion date. Filtering or monitoring must be tested before a new device or service is issued.
- Monitoring alerts and reports must reach identified staff promptly, be reviewed from safeguarding and technical perspectives, use the minimum personal data necessary,

and trigger action under this policy. Staff must not assume that IT support is handling the welfare response.

- Known gaps or outages require documented interim controls such as pausing access, closer supervision, isolating a device or network, or using an approved alternative. High-risk uncontrolled learner access must not continue.

9. Cyber security, accounts and continuity

- Maintain current asset, system, supplier, licence and account registers, including ownership, support status, disposal and criticality.
- Use supported and licensed systems, secure configuration, firewalls, anti-malware and device management. IT support must apply critical or high-risk vulnerability fixes within the relevant DfE standard, normally within 14 days, and act within five working days on specific DfE update instructions.
- Require unique user credentials. Enable multi-factor authentication for staff cloud-service accounts, staff remote access and IT administrative accounts; provide an accessible alternative or organisation-owned authentication method where needed.
- Apply least privilege, separate administrative accounts from daily work, approve privilege changes, review accounts at least termly and disable access immediately when a person leaves or no longer requires it.
- Protect encryption and recovery keys, administrative credentials and emergency access arrangements. Do not store passwords in an unprotected document or share them by ordinary email or message.
- Maintain a documented backup and recovery plan, protect backups from the same incident as live systems, test and log restoration at least termly and review the plan annually. Physical backups must be encrypted, securely held and never taken to a private home.
- Include cyber incidents in business continuity and emergency planning. Safeguarding and essential contact information must remain available through a secure contingency where core systems are unavailable.
- Dispose of devices and media through an authorised secure process that removes data and records disposal. Lost, stolen or unaccounted equipment must be reported immediately.

10. Generative AI and emerging technology

Authorisation first: No child, adult participant, staff member or volunteer may use an AI tool for WSCF activity until the specific tool and use case have been approved. Approval must cover age restrictions, supervision, data protection, safeguarding, intellectual property, accuracy, bias, filtering/monitoring, procurement and accessibility.

- Learner use must be closely supervised and restricted to approved accounts and tasks using products with appropriate safety, filtering and monitoring features.
- Never enter names, images, case histories, safeguarding information, health information, assessment details, confidential business records or identifiable scenarios into a public or unapproved AI service.
- AI output is unverified. A competent person must check accuracy, sources, bias, harmful content, copyright and suitability before it informs learning, communication, assessment or a decision. No significant decision about a person may be delegated to an AI system without the lawful, approved process and meaningful human review.
- Creating sexual, humiliating, threatening or deceptive images, audio, video or impersonations of a real person is prohibited and may be a safeguarding and criminal matter. Deepfakes and synthetic media must be treated according to content and impact, not dismissed as a joke or as unreal.
- AI systems that simulate relationships, counselling or emotional dependency require particular caution. They do not replace a trusted adult, qualified professional, safeguarding response or emergency help.
- WSCF must reassess filtering and monitoring capability before adopting tools that produce real-time, personalised or AI-generated content and must explain any monitoring to users in accessible language.

11. Data, images, remote access and suppliers

- Follow the Data Protection Policy for lawful basis, privacy information, rights, retention, data breaches, complaints, DPIAs, processors and international transfers. This policy does not create a separate data-protection route.
- Use the minimum information needed. Store records in the approved system, not on a personal device, local download, private notebook, removable drive or personal cloud account.
- Photography, video and audio require an authorised purpose, appropriate lawful basis and privacy information, approved equipment, secure transfer and retention controls. Consent for publicity does not authorise safeguarding, learning or identification uses, and vice versa.

- Remote access requires approved equipment and systems, MFA, a private working environment, secure connectivity and protection from household or public viewing. Public or shared computers must not be used for confidential work.
- Before a new app, website, online platform, AI tool, camera, monitoring product or supplier is used, WSCF must assess safeguarding, age suitability, accessibility, security, data processing, contracts, support, exit and evidence-retention needs. A DPIA must be completed where processing is likely to create high risk.
- Contracts must define responsibilities between WSCF, the commissioner and supplier. Outsourcing IT does not outsource WSCF's governance, safeguarding or accountability.

12. Reporting and responding to incidents

Immediate rule: Protect the person first. Do not investigate a safeguarding concern yourself, promise secrecy, confront a suspected person, forward harmful material, or delay a report while trying to prove what happened. Call 999 for immediate danger or a crime in progress, then notify the DSL and Jake Payne as soon as safe.

Situation	Immediate action
Worrying content or contact	Stop or pause access; support the person; note what was seen or said without repeated viewing; report immediately to the DSL; preserve the device and available contextual information.
Nude or sexual image involving a child	Do not ask to see, copy, print, download, screenshot, forward or delete it and do not ask the child to send it. Secure the device without searching it and report immediately to the DSL, who follows current UKCIS and safeguarding guidance.
Adult participant may be at risk	Make the immediate situation safe; report under the Adult Safeguarding Policy; consider capacity, consent and urgent risk; do not let the IT route delay an adult-safeguarding referral.
Phishing, malware or compromised account	Stop interacting; disconnect the affected device from networks if safe but do not wipe or investigate it; use a known safe device to contact Jake Payne and IT support; change credentials only as directed.
Lost, stolen or misdirected information	Contain if safe; do not conceal it; report immediately to Jake Payne under the Data Protection Policy; preserve details needed for breach assessment and safeguarding review.
Filtering or monitoring failure	Stop high-risk access, apply interim supervision or isolation, tell Jake Payne, the DSL and IT support, record the scope and do not restore access until suitable controls are verified.
Illegal content or cyber attack	Do not continue viewing or share material. Preserve systems and logs, follow the cyber incident plan, involve police or specialist reporting routes as directed, and consider safeguarding, data-breach, commissioner and insurer

Situation	Immediate action
	notifications.
Concern about a staff member or owner	Use the allegations/low-level-concerns route in the Safeguarding and Child Protection Policy. If the concern is about the usual recipient, report to the alternative named route or directly to the appropriate external authority.

12.1 Recording and evidence

- Record promptly in factual language: date/time, people involved, exact words where relevant, device/account/service, location, immediate risk, action taken, who was informed and outstanding actions.
- Do not investigate by searching messages, accounts, browser history or cloud storage unless specifically authorised by the DSL or incident lead and legally appropriate. Do not make unnecessary copies of harmful content.
- Preserve potentially relevant logs, emails, URLs, usernames and device details without interacting further with illegal or harmful material. Maintain confidentiality and a clear record of who handled a device or evidence.
- The DSL leads the welfare response; IT support leads technical containment under management direction; Jake Payne coordinates operational, commissioner and data-protection action. These workstreams must share necessary information and not assume another person has completed the report.

13. Training, assurance and review

- All staff and volunteers receive safeguarding training including online safety and filtering/monitoring responsibilities at induction, regular updates as needed and at least annually, plus annual cyber-security and data-protection training relevant to their access.
- Role-specific training is required for the DSL, digital lead, managers, people reviewing alerts, IT support and anyone approving AI, systems, suppliers, communications or media.
- Children and adult participants receive accessible instruction before use and reinforcement matched to their needs and experience. Parents, carers and commissioners receive proportionate information about rules, systems and significant changes.
- Jake Payne will maintain an annual assurance record covering filtering/monitoring, cyber risk, accounts, patches, backups and restore tests, suppliers, incidents and

near misses, training, AI and new technology, user feedback and outstanding actions.

- This policy is reviewed at least annually and sooner following a serious or repeated incident, safeguarding review, technology or supplier change, new AI use, material change in users or provision, commissioner requirement, law or guidance change, or evidence that controls are not working.

Appendix A - Staff immediate-action guide

If this happens	Do now	Do not
A person reports online harm	Listen, reassure, make safe, record exact words, tell the DSL now.	Do not promise secrecy, blame, interrogate or investigate.
Unexpected harmful content appears	Stop access, move the person away, close or lock if safe, report.	Do not keep viewing, screenshot, forward or show colleagues.
Possible child sexual image	Secure device without searching; tell the DSL immediately.	Do not view, copy, print, delete or ask for it to be sent.
Suspicious email or login prompt	Stop; use a safe route to contact IT/Jake; report credentials if entered.	Do not click again, reply, pay, or use contact details in the message.
Device lost or stolen	Report immediately; give last location, time, owner and data likely present.	Do not wait until the end of the day or conceal the loss.
Filtering is not working	Pause learner access; increase direct supervision; alert DSL, Jake and IT.	Do not continue because the activity is planned or assume monitoring will catch it.
Immediate danger/crime in progress	Call 999, make people safe, then notify DSL/management.	Do not seek managerial permission before calling 999.

Appendix B - Annual online-safety and IT assurance record

The completed review is a controlled record. Supporting technical details may be held separately where wider circulation would create a security risk.

Review area	Evidence and minimum question	Owner / date / action
Users and risk profile	Ages, SEND/EAL, vulnerabilities, adult participants, access patterns, locations, off-site use and emerging harms considered?	
Filtering	All connections, devices, apps, profiles, guest/BYOD access and required blocklists tested and logged? Limitations and over-blocking reviewed?	
Monitoring	Alerts reach the right people in time; responsibilities, privacy, escalation and response records tested?	
AI and new technology	Approved tools/use cases, ages, data, human review, synthetic media, personalised content and monitoring capability assessed?	
Cyber risk	Asset/system risks reviewed annually and termly; firewalls, anti-malware, patches, MFA, privileged access and leavers	

Review area	Evidence and minimum question	Owner / date / action
	checked?	
Backups and continuity	Backup plan current; protected copies and termly restore test evidenced; safeguarding continuity available?	
Suppliers and data	Contracts, processors, security, DPIAs, international access, retention, exit and incident support reviewed?	
People and practice	Training complete; acceptable-use rules acknowledged; staff, learner, parent/carer and commissioner feedback considered?	
Incidents and actions	Trends, near misses, complaints, safeguarding/data/cyber actions and overdue improvements reviewed?	
Approval	Review outcome approved, residual risks accepted by an authorised person, and next review/check date set?	

Appendix C - Related policies and authoritative sources

Related WSCF policies

- Safeguarding and Child Protection Policy; Adult Safeguarding Policy; Data Protection Policy; Anti-Bullying Policy; Behaviour Policy; Staff Code of Conduct; Complaints and Concerns Procedure;
- Mobile Phone, Smoking and Vaping Policy; Two-Way Radio Policy and Staff Operating Guide; Emergency Response Plan; Emergency Lockdown Policy; Health and Safety Policy; and
- photography/media, remote-working, business-continuity, retention and supplier procedures where maintained separately.

Authoritative sources checked for this revision

- Department for Education, Keeping Children Safe in Education 2026 (effective 1 September 2026) and KCSIE 2025 during the transition period;
- Department for Education, Filtering and monitoring core standard and Cyber security core standard, updated 24 June 2026;
- Department for Education, Generative artificial intelligence in education and Generative AI product safety standards;
- Department for Education, Non-school alternative provision: voluntary national standards;

- UK Council for Internet Safety, Sharing nudes and semi-nudes: advice for education settings;
- Information Commissioner's Office, Children and the UK GDPR and edtech guidance; and
- National Cyber Security Centre, cyber-security guidance for education and ransomware-resistant backup guidance.

Approval record

Approval	Name / signature	Date
Approved by	Jake Payne	06/08/2026
Policy owner acknowledgement	Jake Payne	06/08/2026
Next scheduled review	August 2027	Earlier if a trigger in section 13 applies