New Pastures Primary School

Online Safety Policy

1	Owned and reviewed by	Principal
3	Approval date	01/09/2026
4	Date of next review	01/09/2027
5	Version number	2
6	Related documents (if applicable)	
7	Applies to	☒ All staff ☐Support staff ☐Teaching staff
8	Available on	☐Trust website ☒School website ☒SharePoint

Venn Academy Trust (VAT) is a charitable company limited by guarantee with registration number 09662303 and Sole Member of the subsidiary company Venn Education Group (VEG). Venn Education Group is a charitable company limited by guarantee with registration number 16743074. Venn wide policies are centrally held policies and are the direct responsibility of VAT. Venn wide policies are created by the VAT Central Team and adopted by the VEG Board.

Contents

1 Aims 3
2 Legislation and guidance 3
3 Roles and responsibilities 3
3.1 The governing board 3
3.2 The principal 3
3.3 The designated safeguarding lead 3
3.4 ICT technical support 4
3.5 All staff and volunteers 4
3.6 Parents and carers 4
3.7 Visitors and community users 4
4 Educating pupils about online safety 4
4.1 Key Stage 1 4
4.2 Key Stage 2 4
4.3 Remote and home learning 5
5 Educating parents and carers about online safety 5
6 Cyber-bullying 5
6.1 Definition 5
6.2 Prevention and response 5
6.3 Examining electronic devices 5
7 Filtering and monitoring using Netsweeper 5
7.1 Purpose and scope 5
7.2 Filtering arrangements 6
7.3 Monitoring and review of alerts 6
7.4 Data protection and confidentiality 6
7.5 Effectiveness checks and assurance 6
8 Pupils using mobile devices in school 7
9 Staff using work devices outside school 7
10 How the school will respond to issues of misuse 7
11 Training 7
12 Links with other policies 7

1 Aims

This policy sets out how New Pastures Primary School provides a safe digital environment, teaches pupils to use technology responsibly, and responds to online safety concerns. Online safety is part of the school's safeguarding arrangements and is everyone's responsibility.

- Set out the principles expected of all members of the school community when using digital technology.
- Safeguard and protect pupils and staff.
- Support staff to use the internet and communication technologies safely and responsibly and to reflect on their own practice.
- Set clear expectations for educational, personal and recreational use of technology.
- Provide clear arrangements for responding to online abuse, cyber-bullying, harmful content and inappropriate contact.
- Ensure that unlawful, unsafe or inappropriate behaviour is addressed and, where necessary, reported to relevant agencies.
- Minimise the risk of misplaced or malicious allegations against adults who work with pupils.

2 Legislation and guidance

This policy has regard to the Department for Education's statutory guidance Keeping Children Safe in Education 2026 and the Department for Education filtering and monitoring standards for schools and colleges. It also reflects current guidance on teaching online safety, relationships and health education, preventing and tackling bullying, searching screening and confiscation, data protection, cyber security and preventing radicalisation.

Relevant legislation includes the Education Act 1996, Education and Inspections Act 2006, Education Act 2011, Equality Act 2010, Data Protection Act 2018 and UK General Data Protection Regulation. The policy also takes account of the National Curriculum computing programmes of study.

3 Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for ensuring that appropriate filtering and monitoring systems are in place, that their effectiveness is reviewed at least annually, and that this policy is implemented. Governors receive assurance through safeguarding reports, monitoring records and discussion with the DSL and school leaders. The governor who oversees online safety is S Hall.

- Read and understand this policy.
- Comply with the acceptable use agreement in appendix 3.
- Ensure appropriate checks and reviews are carried out, while recognising that governors are not expected to perform routine technical checks personally.

3.2 The principal

The principal is responsible for ensuring that staff understand and implement this policy consistently. The principal will:

- Take overall responsibility for online safety, data security and the school's filtering and monitoring arrangements.
- Ensure the school uses an approved filtered internet service and appropriate monitoring technology.
- Ensure staff receive suitable training and know the procedure for responding to a serious online safety incident.
- Receive regular information about online safety concerns and Netsweeper alerts.
- Ensure staff who carry out filtering and monitoring duties are supported and that responsibilities are clearly assigned.

3.3 The designated safeguarding lead

The DSL is Mr B Wray. The deputy DSLs are Miss L Ward and Mrs C Cotton-Bailey. The DSL takes lead responsibility for online safety and filtering and monitoring as safeguarding matters.
The DSL will:

- Work with senior leaders, the Trust and technical support to address online safety issues and incidents.
- Ensure online safety incidents and safeguarding-related Netsweeper alerts are reviewed, recorded and acted upon.
- Ensure cyber-bullying is addressed under the Behaviour Policy and safeguarding procedures.
- Provide staff training and updates and ensure online safety education is embedded across the curriculum.
- Liaise with parents, the local authority, children's social care, the police and other agencies when necessary.
- Report themes, trends, serious incidents and assurance information to leaders and governors without disclosing unnecessary personal information.
- Keep knowledge current in relation to harmful content, grooming, child-on-child abuse, cyber-bullying, extremist material, sexual harassment, online exploitation, artificial intelligence and emerging technology.

3.4 ICT technical support

The school's ICT technical support provider, Alamo, works with the school and Trust to:

- Maintain appropriate filtering, monitoring, security, anti-malware and account controls.
- Implement authorised changes to Netsweeper policies, block lists and allow lists.
- Support checks that filtering works on school networks, devices and relevant locations.
- Investigate technical concerns, attempted bypassing, malware and compromised accounts.
- Provide technical information and reports to authorised school staff while protecting confidentiality.

Technical support does not make safeguarding decisions. Safeguarding concerns and alerts are referred to the DSL or a deputy DSL.

3.5 All staff and volunteers

- Read, understand and implement this policy and the relevant acceptable use agreement.
- Maintain active supervision when pupils use technology; filtering and monitoring do not replace staff vigilance.
- Report online safety concerns immediately to the DSL or a deputy DSL and record safeguarding concerns on CPOMS in line with school procedures.
- Do not investigate a safeguarding concern beyond what is necessary to establish immediate safety and preserve evidence.
- Report over-blocking, under-blocking, technical faults or suspected attempts to bypass controls.
- Model safe, lawful and professional technology use.

3.6 Parents and carers

- Raise concerns or questions with the school promptly.
- Help their child understand and follow the pupil acceptable use agreement.
- Work with the school when an online concern affects a child's safety, welfare or behaviour.

3.7 Visitors and community users

Visitors and community users who access school technology or internet services will be made aware of the relevant expectations and, where appropriate, will agree to the acceptable use agreement in appendix 3.

4 Educating pupils about online safety

Online safety is taught through computing, relationships and health education, assemblies and other subjects where relevant. Teaching is age appropriate, revisited regularly and responsive to new risks and local concerns.

4.1 Key Stage 1

- Use technology safely and respectfully and keep personal information private.
- Recognise when content or contact may be unsafe or upsetting.
- Know how and where to ask for help and report a concern.

4.2 Key Stage 2

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Understand how information and data may be shared and used online.

- Think critically about online friendships, sources, algorithms, advertising, AI-generated content and information that may be false or misleading.
- Recognise harmful content, contact and conduct, and use a range of reporting routes.

The school will teach pupils that people may behave differently or pretend to be someone else online; that the same expectations of respect apply online and offline; and how to respond safely to contact from adults or others they do not know.

4.3 Remote and home learning

Pupils are expected to follow the same acceptable use principles when learning remotely. School systems and accounts must be used only for their intended educational purpose.

5 Educating parents and carers about online safety

The school raises awareness through letters, Class Dojo, the school website, meetings and targeted communication following emerging concerns. Advice may include age restrictions, privacy, gaming, social media, cyber-bullying, harmful content, online exploitation, parental controls and reporting routes. Parents and carers should raise concerns with the principal or DSL.

6 Cyber-bullying

6.1 Definition

Cyber-bullying is bullying carried out through digital technology, including social media, messaging, games and shared content. It may include repeated intentional harm where there is an imbalance of power. A single harmful online incident may still require a safeguarding or behaviour response even when it does not meet the definition of bullying.

6.2 Prevention and response

- Teach pupils what cyber-bullying is, how to report it and how to support others.
- Discuss respectful online behaviour through the curriculum and assemblies.
- Respond under the Behaviour Policy and safeguarding procedures, including child-on-child abuse procedures where relevant.
- Contain harmful material where reasonably possible and preserve evidence appropriately.
- Consider support for the child harmed, the child responsible and other affected pupils.
- Refer suspected criminal or illegal content to the police or another appropriate agency where necessary.

6.3 Examining electronic devices

Searching, screening, confiscation and examination of data will be carried out only in accordance with current Department for Education guidance and the school's Behaviour Policy. Staff must involve the DSL or a senior leader when material may be illegal, indecent, safeguarding-related or evidence of an offence. Staff must not view, copy, print or share a nude or semi-nude image of a child. Such incidents must be referred immediately to the DSL and handled under safeguarding procedures.

7 Filtering and monitoring using Netsweeper

7.1 Purpose and scope

The school uses Netsweeper as its technical web filtering and monitoring system. Filtering is preventative: it restricts access to illegal, inappropriate and potentially harmful content. Monitoring is reactive: it provides information or alerts about activity that may indicate risk. Netsweeper supports, but does not replace, safe system design, staff supervision, education and professional judgement. Controls apply to school internet access and school-managed devices where technically configured.

The school sets clear expectations for any device or connection on which normal filtering and monitoring is not available. Staff must not use an unfiltered connection to enable pupil access unless a specific risk assessment and suitable safeguards are in place.

7.2 Filtering arrangements

- Netsweeper blocks categories and sites associated with illegal content, child sexual abuse, pornography, violence, hate, extremism, gambling, drugs, malware, phishing, anonymisers and other material assessed as unsuitable.
- Safe search and other age-appropriate platform controls are enabled where available.
- Filtering settings are differentiated where appropriate by user, device or age, without unreasonably restricting teaching and learning.
- Requests to unblock or block content are considered by authorised staff. Decisions take account of curriculum need, age, safeguarding risk and data protection. Changes are implemented by authorised technical support and recorded.
- Suspected bypassing, use of proxy or VPN services, or repeated attempts to reach blocked material are investigated.

7.3 Monitoring and review of alerts

Netsweeper produces reports and alerts for activity associated with safeguarding or misuse. Authorised leaders review alerts each school day, with high-risk alerts considered as soon as practicable. Access is limited to staff who require it for safeguarding, leadership or technical support.

When an alert is received, the school will:

Step	Stage	School action
1	Triage	Check the alert category, severity, user, device, time, search terms or URL and available context. Consider whether the activity may be accidental, curriculum-related, a false positive or an indicator of harm.
2	Safeguard	If there may be immediate risk, ensure the pupil or adult is safe and inform the DSL or a deputy DSL without delay.
3	Establish context	Speak with relevant staff and, where appropriate, the pupil. Staff will use open, non-leading questions and will not conduct an unnecessary investigation.
4	Record	Record the outcome and rationale in the monitoring record. Safeguarding concerns are recorded on CPOMS; behaviour incidents are recorded in accordance with the Behaviour Policy.
5	Act	Actions may include pastoral support, parental contact where safe and appropriate, curriculum input, a proportionate behaviour response, account or device restrictions, a filtering change, referral to children's social care, Prevent, the police or another agency.
6	Close and follow up	Record who reviewed the alert, actions taken, referrals, technical changes and any follow-up date. Alerts with no safeguarding concern are closed with a brief rationale rather than deleted without review.

7.4 Data protection and confidentiality

Monitoring information is processed for safeguarding, security and the proper operation of school systems. Access is proportionate and role based. Records are retained and shared in line with the school's data protection, safeguarding and retention arrangements. Monitoring will not be used for indiscriminate or covert surveillance unrelated to a legitimate school purpose.

7.5 Effectiveness checks and assurance

- The effectiveness of filtering and monitoring is reviewed formally at least once each academic year and after a serious incident or significant change.
- Checks include school devices, relevant user groups, wired and wireless networks, both school sites and other relevant locations. The date, scope, outcome and remedial action are recorded.
- The DSL, principal, Trust and technical support consider pupil risk profiles, SEND, age, curriculum needs, remote access, AI tools and technologies that may reduce the effectiveness of controls.

- Themes and significant concerns are reported to governors. Personal details are shared only where necessary.
- If filtering or monitoring is unavailable, the school will restrict or stop affected internet use unless safe alternative arrangements are in place.

8 Pupils using mobile devices in school

Year 5 and Year 6 pupils who walk to or from school may bring a mobile phone when parental permission and school arrangements allow. Phones must be handed in and stored securely as directed and must not be used during the school day. Misuse will be addressed under the Behaviour Policy and may result in the privilege being withdrawn.

9 Staff using work devices outside school

- Do not install unauthorised software or use the device in breach of the staff acceptable use agreement.
- Keep devices secure, encrypted where provided, password protected and physically safe.
- Do not share passwords or allow family members or others to use work accounts or devices.
- Use only approved storage and transfer methods for personal or confidential information.
- Report loss, theft, suspected compromise or security concerns immediately.
- Use work devices for authorised professional activity in accordance with Trust and school requirements.

10 How the school will respond to issues of misuse

Responses will reflect the individual circumstances, the nature and seriousness of the incident, any safeguarding risk and the needs of those involved. Actions will be lawful, proportionate, educational and consistent with the Behaviour Policy, safeguarding procedures, Staff Code of Conduct and disciplinary procedures.

The school may provide support, restorative work or additional teaching; contact parents or carers; restrict access to an account, device or service; preserve evidence; make a filtering change; apply a behaviour consequence; begin a staff process; or refer to children's social care, the police, Prevent or another relevant agency. Suspected illegal content will not be unnecessarily viewed, copied or circulated.

11 Training

- New staff receive online safety, acceptable use, filtering and monitoring information during induction.
- All staff receive safeguarding and online safety training at least annually, with updates during the year when risks, systems or procedures change.
- Staff who review Netsweeper alerts receive role-specific training in triage, safeguarding response, recording, confidentiality and escalation.
- The DSL and deputy DSLs maintain their knowledge through statutory safeguarding training and regular updates.
- Pupils and parents receive information appropriate to their needs.

12 Links with other policies

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct and disciplinary procedures
- Data Protection Policy, privacy notices and records retention arrangements
- Complaints Procedure
- Acceptable Use Agreements
- Relationships and Health Education Policy
- Prevent risk assessment and emergency or critical incident arrangements