



Online Safety Policy

Signed by headteacher: *A Hughes*

Signed by Chair of Governors: *David Bradley*

Date of Approval: September 2026

Date for review: September 2027

This policy will also be reviewed following a serious online-safety incident, a significant change to the school's technology or provision, an identified weakness, or a change to relevant legislation or statutory guidance.



Contents

Statement of intent	2
1. Legal framework	3
2. Roles and responsibilities	4
3. Managing online safety	5
4. Cyberbullying	6
5. Child-on-child sexual abuse and harassment	6
6. Grooming and exploitation	7
7. Mental health	7
8. Online hoaxes and harmful online challenges	8
9. Cyber-crime	8
10. Online safety training for staff	9
11. Online safety and the curriculum	9
12. Use of technology in the classroom	10
13. Use of smart technology	10
14. Working with parents and carers	11
15. Internet access	11
16. Filtering and monitoring online activity	12
17. Network security	12
18. Emails	13
19. Generative artificial intelligence (AI)	13
20. Social networking	14
21. The school website	14
22. Use of devices	15
23. Remote learning	15
24. Monitoring and review	16

Statement of intent

Bitterne Manor Primary School recognises online safety as an essential part of safeguarding. Technology provides valuable opportunities for teaching, learning and communication, but it can also expose pupils and staff to harm.

The school's approach addresses four areas of online risk:

- **Content:** exposure to illegal, inappropriate or harmful material.
- **Contact:** harmful interaction with others, including bullying, grooming and exploitation.
- **Conduct:** behaviour that causes harm, including abuse, inappropriate sharing and cyberbullying.
- **Commerce:** risks including scams, phishing, inappropriate advertising and online gambling.

Online safety is addressed through the curriculum, staff training, safeguarding procedures, appropriate filtering and monitoring, secure technology systems and work with parents and carers.

The school recognises that online harm may occur inside or outside school and on school-owned or personal devices. Relevant concerns will be managed in accordance with the Child Protection and Safeguarding Policy.

The school will take a child-centred and proportionate approach. Pupils will be listened to, supported and encouraged to report concerns without fear of blame. Particular consideration will be given to pupils who may be more vulnerable to online harm, including pupils with SEND.

This policy aims to ensure that:

- pupils use technology safely, responsibly and respectfully;
- pupils learn how to recognise risks and seek help;
- staff understand and fulfil their online-safety responsibilities;
- appropriate filtering, monitoring and security arrangements are maintained; and
- online-safety concerns are identified, reported and managed promptly.

1. Legal framework

This policy has due regard to relevant legislation and guidance, including:

- Children Act 1989 and Children Act 2004
- Education Act 2002
- Equality Act 2010
- Data Protection Act 2018 and UK GDPR
- Computer Misuse Act 1990
- Protection from Harassment Act 1997
- Sexual Offences Act 2003
- Voyeurism (Offences) Act 2019
- Counter-Terrorism and Security Act 2015
- Online Safety Act 2023
- DfE, Keeping Children Safe in Education 2026
- DfE, Working Together to Safeguard Children
- DfE, Filtering and Monitoring: Core Standard
- DfE, Cyber Security: Core Standard
- DfE, Teaching Online Safety in Schools
- DfE, Relationships Education, Relationships and Sex Education and Health Education statutory guidance
- DfE, Searching, Screening and Confiscation
- DfE, Harmful Online Challenges and Online Hoaxes
- DfE guidance on generative artificial intelligence in education
- UKCIS, Sharing Nudes and Semi-Nudes: Advice for Education Settings
- UKCIS, Education for a Connected World
- Prevent duty guidance

This policy should be read alongside the school's:

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Behaviour Policy
- Anti-Bullying Policy
- Acceptable Use Agreements
- Relationships and Health Education Policy
- Computing Policy
- Data Protection Policy
- Staff ICT and Electronic Devices Policy
- Pupils' Personal Electronic Devices Policy
- Cyber Security Policy
- Cyber Response Plan
- Remote Education Policy
- Safe Use of AI Policy

Where legislation or statutory guidance changes, the school will follow the most recent requirements and update this policy as soon as practicable.

2. Roles and responsibilities

The governing board will:

- ensure that online safety is included within the school's safeguarding arrangements;
- ensure that appropriate filtering and monitoring systems are in place;
- appoint a governor and an SLT member with responsibility for filtering and monitoring;
- receive assurance that filtering and monitoring arrangements are effective;
- receive and scrutinise termly assurance about online safety, including significant incidents, filtering and monitoring, staff training, curriculum implementation and outstanding improvement actions;
- ensure that staff receive appropriate online-safety training; and
- review this policy at least annually.

The **headteacher** will:

- ensure that this policy is implemented consistently;
- ensure that online-safety responsibilities are clearly assigned;
- provide staff with appropriate training, time and resources;
- ensure that significant risks and incidents are addressed; and
- report relevant risks and assurance to the governing board.

The **SLT lead** for filtering and monitoring will:

- oversee the school's compliance with the DfE filtering and monitoring standards;
- ensure that filtering and monitoring arrangements meet the school's needs;
- document significant decisions about what is blocked or allowed;
- lead the annual review with the DSL and IT support; and
- report findings and required actions to the headteacher and governing board.

The **designated safeguarding lead** will:

- take lead responsibility for online safety as part of safeguarding;
- understand the school's filtering and monitoring arrangements;
- respond to safeguarding concerns identified through monitoring;
- ensure that staff know how to recognise and report online-safety concerns;
- maintain appropriate records and identify patterns or emerging risks;
- consider the additional online vulnerabilities of individual pupils and groups;
- liaise with parents, children's social care, the police and other agencies where appropriate.
- provide the governing board with a termly online-safety report covering significant incidents and emerging risks, filtering and monitoring assurance, staff training, curriculum implementation and progress against identified actions;

IT support will:

- maintain the school's filtering, monitoring and cyber-security systems;
- carry out and record agreed checks;
- report technical failures or weaknesses promptly;
- ensure that only authorised users can change system settings;
- provide relevant monitoring information to the DSL; and
- support the annual filtering and monitoring review.

All staff will:

- follow the Staff Code of Conduct and Acceptable Use Agreement;
- model safe, responsible and professional use of technology;
- supervise pupils' use of technology appropriately;
- use authorised systems and protect passwords and personal information;
- remain alert to signs that a pupil may be at risk online;
- report safeguarding concerns without delay; and
- report filtering failures, security weaknesses or suspected cyber incidents promptly.

Pupils will be taught and expected to:

- follow the school's Acceptable Use Agreement;
- use technology safely, responsibly and respectfully;
- protect personal information and respect the privacy of others;
- report harmful content or behaviour to a trusted adult;
- continue asking for help until they receive it; and
- not attempt to bypass the school's security or filtering controls.

Parents and carers will be encouraged to:

- discuss safe and responsible technology use with their child;
- support the school's online-safety expectations;
- use age-appropriate supervision and parental controls; and
- inform the school when an online incident may affect their child's safety, wellbeing or education.

3. Managing online safety

Online safety is part of the school's wider safeguarding arrangements. The school will maintain an annual online-safety risk assessment informed by:

- the ages, needs and experiences of pupils;
- safeguarding and behaviour concerns;
- pupil voice;
- filtering and monitoring information;
- new technology and emerging online harms; and
- lessons learned from incidents.

Actions identified through the risk assessment will be recorded, assigned and reviewed.

Reporting concerns

Any online-safety concern involving a pupil must be reported to the DSL or a deputy DSL without delay and recorded in accordance with the Child Protection and Safeguarding Policy.

Staff receiving a disclosure will:

- listen calmly and take the concern seriously;
- avoid blame, judgement and promises of confidentiality;
- make an accurate record using the pupil's own words where possible; and
- explain that information will be shared with those who need it to help keep the pupil or others safe.

Staff must not investigate the concern, contact an alleged perpetrator or search a pupil's device unless authorised under an approved school procedure.

Where an incident involves nudes or semi-nudes, staff must not view, copy, save, print, forward or ask a pupil to share the imagery. The device should be secured and the matter referred immediately to the DSL.

Responding to concerns

The DSL will assess each concern and decide what action is required. This may include:

- providing support and safety planning;
- involving parents or carers;
- preserving relevant evidence;
- making a referral to children's social care or the police; or
- seeking advice from the local authority or another appropriate agency.

The school will take a child-centred and proportionate approach. A pupil will receive safeguarding support even where they may also have breached a school rule or used an age-restricted service. Any disciplinary response will be considered separately and will not replace safeguarding action.

The school may respond to incidents occurring outside school or on personal devices where they create a safeguarding risk, affect a pupil's welfare or education, or adversely affect the school community.

Parents and carers will normally be informed unless doing so may place a child at greater risk or conflict with advice from children's social care or the police. Decisions and reasons will be recorded.

Concerns about the online conduct of a member of staff, volunteer, contractor or supply worker will be managed under the school's allegations and low-level-concerns procedures. Concerns about the headteacher will be reported to the chair of governors.

The DSL will monitor recorded incidents to identify patterns, emerging risks and any necessary changes to teaching, staff training or technical controls.

4. Cyberbullying

Cyberbullying is bullying carried out through digital technology. It may include:

- abusive, threatening or discriminatory messages;
- spreading rumours or sharing embarrassing content;
- deliberately excluding someone from an online group;
- impersonating another person or using their account;
- sharing images or information without consent; and
- repeated harassment through social media, messaging, gaming or other online services.

The school recognises that cyberbullying may occur inside or outside school, can continue at any time and may reach a wide audience. Some pupils, including pupils with SEND and those experiencing prejudice or discrimination, may be particularly vulnerable.

Cyberbullying will not be tolerated. Concerns will be managed under the Anti-Bullying and Behaviour Policies and, where there is a safeguarding risk, the Child Protection and Safeguarding Policy.

Pupils will be encouraged to:

- avoid responding or retaliating;
- preserve relevant evidence where it is safe to do so;
- use reporting and blocking tools; and
- tell a trusted adult and continue asking for help until action is taken.

The school will support affected pupils, consider the needs of any pupil responsible for the behaviour and work with parents, platforms or external agencies where appropriate.

5. Child-on-child sexual abuse and harassment

Technology may be used to facilitate child-on-child sexual abuse or harassment. This may occur inside or outside school and can include:

- unwanted sexual comments or messages;
- sexualised bullying, threats or coercion;
- pressure to create or share sexual images;
- consensual or non-consensual sharing of nudes or semi-nudes;
- sharing sexual or embarrassing content without consent;
- upskirting;
- digitally altered or AI-generated sexualised images; and
- abuse within intimate personal relationships.

The school has a zero-tolerance approach to sexual abuse and harassment. Such behaviour will not be dismissed as joking, banter or part of growing up.

All concerns will be reported to the DSL and managed under the Child Protection and Safeguarding Policy. The procedures in Section 3 will be followed where nudes or semi-nudes are involved.

The school will:

- listen to and support affected pupils without blame;
- consider the wishes and safety of the pupil who has experienced harm;
- assess risks to all pupils involved;
- consider appropriate support for any pupil alleged to have caused harm;
- prevent further contact, sharing or harassment where possible; and
- involve parents, children's social care, the police or other agencies where appropriate.

Safeguarding action will be considered separately from any action taken under the Behaviour Policy. Incidents occurring outside school will be addressed where they affect the safety, wellbeing or education of pupils.

6. Grooming and exploitation

Grooming is the process of building a relationship with a child, or with people around a child, to gain access, trust or control for the purpose of abuse or exploitation. It may occur entirely online or across online and offline environments.

Online grooming may be linked to:

- sexual abuse or exploitation;
- criminal exploitation, including county lines;
- financial exploitation or sextortion;
- radicalisation;
- trafficking; or
- pressure to share information, images, money or access to accounts.

Online grooming may also be used to draw a pupil towards extremist ideologies or support for terrorism. Staff must report concerns about online radicalisation to the DSL without delay. The DSL will assess the concern under the Child Protection and Safeguarding Policy and Prevent Duty arrangements and consider whether advice or a referral to the local authority Prevent team or Channel programme is required.

Those responsible may disguise their identity, pretend to share a pupil's interests, offer gifts or attention, seek to move conversations to private channels, encourage secrecy or use threats and blackmail.

Pupils will be taught in an age-appropriate way to recognise unsafe contact, protect personal information, question online identities, refuse requests and seek help from a trusted adult.

Staff will remain alert to indicators of grooming or exploitation, including unexplained gifts or money, secrecy about online activity, contact with unknown individuals, changes in behaviour, fear, withdrawal or possession of additional devices.

Any concern about grooming or exploitation must be reported to the DSL without delay and managed under the Child Protection and Safeguarding Policy. The DSL will consider the need for immediate protection, preservation of evidence and referral to children's social care, the police, CEOP or other relevant agencies.

7. Mental health

Online experiences can have a positive or negative effect on pupils' mental health and wellbeing. Potential risks include:

- cyberbullying, harassment or exclusion;
- pressure arising from comparison, popularity or appearance;
- excessive or disruptive use of technology;
- sleep disruption;
- exposure to distressing content; and
- content that promotes self-harm, suicide or eating disorders.

Changes in a pupil's online behaviour may also indicate that they are experiencing harm. Staff will remain alert to signs such as withdrawal, distress, disrupted sleep, secrecy, anxiety or significant changes in technology use.

Pupils will be taught age-appropriate strategies for maintaining healthy online habits, managing screen time, seeking reliable information and asking for help.

Staff must report concerns about a pupil's mental health or exposure to harmful content to the DSL in accordance with the Child Protection and Safeguarding Policy. Concerns involving self-harm, suicide or immediate danger will be treated as urgent safeguarding matters.

8. Online hoaxes and harmful online challenges

Online hoaxes and challenges may encourage frightening, dangerous or harmful behaviour. Publicising them unnecessarily can increase curiosity and exposure.

The school will take a measured and proportionate approach. Before communicating with pupils or parents, the DSL will consider:

- whether the concern is genuine and relevant to the school;
- the possible risk to pupils;
- whether communication could unintentionally promote the content; and
- advice from reliable safeguarding sources.

Communications will avoid naming, describing or linking to harmful content unless this is necessary to keep pupils safe. They will focus on safe behaviour, reporting concerns and seeking help.

Pupils will be taught not to participate in or share harmful challenges, to question alarming online claims and to tell a trusted adult if they encounter concerning content.

Any concern that a pupil has taken part in, promoted or been harmed by an online challenge will be reported to the DSL and managed under the Child Protection and Safeguarding Policy. Emergency assistance will be sought where there is an immediate risk of harm.

9. Cyber-crime

Cybercrime includes criminal activity involving computers, networks or online services. Examples include:

- accessing accounts or systems without permission;
- creating or spreading malware;
- disrupting a network or online service;
- stealing data or passwords;
- phishing, fraud and online scams; and
- using technology to facilitate other offences.

The school recognises that pupils may become involved through curiosity, coercion, exploitation or a lack of understanding about the law. A pupil showing a strong interest in testing or bypassing systems will be supported to develop those skills safely and legally.

Pupils and staff must report suspected cybercrime, security breaches, phishing or unusual system activity promptly to IT support and the DSL.

Suspected incidents will be managed under the school's Cyber Response Plan. Staff must not investigate, delete evidence or attempt to resolve a suspected attack unless authorised to do so.

The school will take immediate steps to protect pupils, information and systems and will seek advice or report the incident to the appropriate authority where necessary.

10. Online safety training for staff

Online safety will form part of safeguarding and child-protection training for all staff at induction. Staff will receive updates at least annually and more frequently where risks, guidance or school arrangements change.

Training will ensure that staff understand:

- how technology can facilitate abuse, exploitation and bullying;
- the four areas of online risk: content, contact, conduct and commerce;
- indicators that a pupil may be unsafe online;
- how to respond to a disclosure or concern;
- their responsibilities for filtering and monitoring;
- how to report filtering failures or cyber-security concerns;
- the additional risks that some pupils, including those with SEND, may face; and
- the safe and appropriate use of emerging technology, including generative AI.

The DSL will maintain a record of training and identify further training needs through safeguarding concerns, staff feedback, monitoring information and changes to guidance.

Governors and staff with specific responsibilities for online safety, filtering, monitoring or IT security will receive training appropriate to their roles.

11. Online safety and the curriculum

Online safety is taught through computing, Relationships and Health Education, PSHE and the wider curriculum. Teaching is age-appropriate, progressive and responsive to pupils' needs and experiences.

The school uses Purple Mash 2BeSafe from Reception to Year 6 as its principal planned online-safety programme. It is based on the UK Council for Internet Safety's Education for a Connected World framework and covers:

- self-image and identity;
- online relationships;
- online reputation;
- online bullying;
- managing online information;
- health, wellbeing and lifestyle;
- privacy and security; and
- copyright and ownership.

2BeSafe supports the relevant online elements of statutory Relationships and Health Education. It does not replace the school's wider computing, PSHE, safeguarding or Relationships and Health Education provision.

Teachers will adapt and supplement the programme to reflect pupils' ages and needs, including the needs of pupils with SEND, risks identified by the school and emerging technologies or online harms.

Teaching will help pupils to:

- recognise harmful content, contact and behaviour;
- evaluate the reliability of online information;
- protect their privacy and personal information;
- understand consent, respectful behaviour and healthy boundaries;
- recognise scams, manipulation and persuasive design;
- develop healthy technology habits; and
- report concerns and seek help from a trusted adult.

Teaching will also address:

- misinformation, disinformation, conspiracy theories, manipulated media and AI-generated content, including how to check the source, purpose, evidence and reliability of online information;
- the ways algorithms, persuasive design and repeated exposure may influence what pupils see and believe;
- online radicalisation and extremist content, including grooming, manipulation, closed groups, harmful narratives and the importance of reporting concerning material or contact;
- financial and commercial risks, including phishing, scams, fraudulent offers, subscription traps, in-app purchases, loot boxes, gambling-style features, influencer advertising and pressure to spend or share financial information; and
- how to use platform-reporting tools, seek help from a trusted adult and avoid sharing or amplifying harmful content.

Teachers will check external resources before use and consider whether sensitive content may affect individual pupils. Safeguarding concerns or disclosures arising during lessons will be reported in accordance with the Child Protection and Safeguarding Policy.

Teachers will use the assessment and reflection opportunities within 2BeSafe to check pupils' knowledge and ability to apply safe behaviours. The computing or curriculum leader, working with the DSL, will monitor coverage, progression and pupils' understanding.

Parents and carers will be informed about the school's use of 2BeSafe and supported to reinforce online-safety messages at home.

12. Use of technology in the classroom

Technology used in teaching will be appropriate to pupils' ages, needs and learning objectives. Pupils will receive suitable supervision and guidance when using online resources.

Before using or recommending a website, application or online service, staff will consider:

- its educational purpose and suitability;
- age restrictions and terms of use;
- privacy and data-protection requirements;
- advertising, communication and sharing features;
- accessibility and the needs of pupils with SEND; and
- any risk of harmful or inappropriate content.

New online services that require pupil accounts or process personal data must be approved in accordance with the school's data-protection and procurement procedures.

Staff will use school-approved accounts and systems and will not require pupils to provide unnecessary personal information. Copyright and licensing requirements will be followed.

Any unsuitable content, safeguarding concern or failure of filtering or monitoring discovered during a lesson will be reported promptly.

13. Use of smart technology

Smart technology includes mobile phones, smartwatches and other personal devices capable of connecting to the internet, recording, communicating or sharing information.

Pupils must follow the school's rules for personal devices. They will not use smart technology during lessons or elsewhere on the school site unless specifically authorised by a member of staff.

Reasonable exceptions may be agreed for medical, safeguarding, accessibility or SEND-related needs.

Pupils will be taught that personal devices may:

- provide unfiltered internet access through mobile networks;
- enable inappropriate recording or sharing;
- disclose personal information or location;
- disrupt learning; or
- be used to bully, harass or contact others inappropriately.

Misuse will be managed under the Behaviour Policy and, where appropriate, the Child Protection and Safeguarding Policy. Searching, screening or confiscation will only take place in accordance with the school's approved procedures.

Staff must use personal and school-owned smart technology in accordance with the Staff Code of Conduct and Staff Acceptable Use Agreement. Personal devices must not be used to photograph, record or store information about pupils unless specifically authorised.

14. Working with parents and carers

The school will work with parents and carers to promote safe and responsible use of technology at school and at home.

Parents and carers will be provided with information about:

- the school's online-safety expectations;
- the pupil Acceptable Use Agreement;
- age restrictions, parental controls and privacy settings;
- emerging online risks and harmful content;
- maintaining healthy technology habits; and
- how to report a concern or obtain support.

Information may be shared through the school website, newsletters, workshops, meetings or targeted communications.

Communications about specific online risks will be proportionate and will avoid unnecessarily naming, describing or linking to harmful content.

Parents and carers will be encouraged to talk openly with their children about online experiences and to respond calmly when a child seeks help. They should inform the school where an online incident may affect their child's safety, wellbeing or education.

The school may provide information and signposting but cannot monitor or control pupils' internet use outside school. Safeguarding concerns reported by parents or carers will be managed under the Child Protection and Safeguarding Policy.

15. Internet access

Access to the school's internet and systems will be appropriate to the user's role, age and needs. Staff and pupils must follow the relevant Acceptable Use Agreement. Visitors and contractors will be provided with controlled access where required and must follow the school's conditions of use.

The school will:

- use individual accounts where appropriate;
- provide suitable supervision and guidance for pupils;
- restrict access according to age and role;
- use a separate or controlled network for visitors where possible; and
- remove or amend access promptly when it is no longer required.

Users will be informed that activity on school networks and school-managed devices may be filtered and monitored for safeguarding, security and operational purposes.

Personal mobile networks may bypass the school's filtering and monitoring arrangements. Personal devices must therefore be used in accordance with Section 13 and the relevant school policies.

Filtering and monitoring do not replace appropriate supervision, education or professional judgement.

16. Filtering and monitoring online activity

The governing board will ensure that the school has filtering and monitoring arrangements that meet the DfE's Filtering and Monitoring: Core Standard and the safeguarding needs of its pupils.

The school will:

- assign an SLT member and governor responsibility for filtering and monitoring;
- block harmful and inappropriate content without unreasonably affecting teaching and learning;
- maintain an effective monitoring strategy;
- consider pupils' ages, needs and risk profiles, including pupils who may be more vulnerable;
- consider school-managed devices used away from the school site;
- establish expectations for personal or other devices that are not covered by the school's systems; and
- inform users, parents and carers about the school's arrangements.

The responsible SLT member will lead a formal review at least once every academic year with support from the DSL and IT support. The review will include:

- checks that filtering and monitoring operate on all relevant internet-connected devices and in all relevant locations;
- consideration of safeguarding incidents, monitoring reports and emerging risks;
- testing of filtering categories and reporting routes;
- consideration of over-blocking and its effect on teaching and safeguarding; and
- a record of findings, actions, responsible persons and completion dates.

IT support will complete and record technical checks of the school's filtering and monitoring provision at least monthly and following any significant change to the network, filtering service, monitoring service or device configuration.

Checks will include, as appropriate:

- confirmation that filtering operates on all relevant internet-connected devices, networks and locations;
- testing of agreed categories of harmful and inappropriate content;
- confirmation that monitoring alerts are generated, received and escalated correctly;
- consideration of school-managed devices used away from the school site;
- identification of over-blocking that may adversely affect teaching, learning or safeguarding; and
- confirmation that identified weaknesses have been resolved.

The responsible SLT member will review the record of checks at least termly with the DSL and IT support. Any failure that may expose a pupil to harm must be reported immediately to the DSL and headteacher. Findings, actions, responsible persons and completion dates will be recorded.

A formal review of the effectiveness of filtering and monitoring will continue to take place at least once every academic year.

Changes to filtering or monitoring settings must be authorised, risk-assessed where appropriate and recorded. Safeguarding needs will take priority when urgent action is required.

Monitoring information will be reviewed by appropriately trained and authorised staff. Safeguarding concerns identified through monitoring will be referred to the DSL and managed under the Child Protection and Safeguarding Policy.

Monitoring will be necessary, proportionate and transparent. Information will be accessed, retained and shared in accordance with data-protection and safeguarding requirements.

Where suspected illegal content is encountered, staff must not investigate further, copy or share it. The matter will be secured and referred immediately to the DSL and IT support, who will seek advice or report it to the appropriate agency.

17. Network security

The school will maintain proportionate cyber-security measures to protect pupils, staff, systems and information.

These will include:

- supported and securely configured devices and software;
- prompt installation of security updates;
- firewalls, anti-malware and other appropriate protections;
- individual user accounts and role-based access;
- strong, unique passwords or passphrases;
- multi-factor authentication where required;
- secure, tested backups;
- restricted administrator privileges; and
- procedures for responding to and recovering from cyber incidents.

Accounts and access permissions will be reviewed regularly and removed or amended promptly when no longer required. Users must lock devices when unattended and must not share accounts or passwords.

Software, applications and browser extensions may only be installed by authorised users. School information must be stored using approved systems.

Suspected malware, unauthorised access, lost devices, data breaches or other cyber-security concerns must be reported immediately. Incidents will be managed under the school's Cyber Response Plan. Detailed technical arrangements are set out in the Cyber Response Plan.

18. Emails

School business must be conducted using approved accounts and communication systems. Personal email or messaging accounts must not be used to communicate with pupils or to store or transfer school information.

Users will:

- protect their account and login details;

- check recipients carefully before sending information;
- use appropriate security when sharing personal or sensitive information;
- avoid opening unexpected links or attachments;
- report suspected phishing, malware or inappropriate messages promptly; and
- communicate professionally and in accordance with the Staff Code of Conduct.

Pupils will only use school-provided communication accounts where these have been approved for their age and educational needs. Their use will be appropriately supervised, filtered or monitored.

Staff must not communicate privately with pupils through personal email, social media or messaging services. Approved school channels must be used.

The school may filter and monitor communications sent through its systems for safeguarding, security and operational purposes. Users will be informed of this monitoring.

Suspected cyber incidents arising through email or electronic communication will be managed under the Cyber Response Plan. Safeguarding concerns will be reported to the DSL.

19. Generative artificial intelligence (AI)

Generative AI may support teaching and administration when used safely, lawfully and appropriately. It must not replace professional judgement or responsibility.

Only school-approved AI tools and accounts may be used for school purposes. Before approval, the school will consider:

- age restrictions and terms of use;
- data protection and security;
- filtering and monitoring;
- copyright and ownership;
- the risk of inaccurate, biased or harmful output; and
- whether a data protection impact assessment is required.

Staff and pupils must not enter personal, confidential or special-category information into an AI tool unless its use has been specifically approved for that purpose.

AI-generated content must be checked by a responsible member of staff before it is used or shared. Staff remain accountable for its accuracy, suitability, fairness and accessibility.

Pupils will only use generative AI when authorised and appropriately supervised. They will be taught to question outputs, protect personal information, acknowledge its use where required and report harmful or concerning content.

Safeguarding concerns involving AI, including the creation of abusive, deceptive or sexualised content, will be reported immediately to the DSL.

20. Social networking

Staff and pupils must use social media in accordance with the relevant Acceptable Use Agreement, Staff Code of Conduct and Behaviour Policy.

Staff must:

- maintain appropriate professional boundaries;
- not communicate with pupils through personal accounts;
- not accept pupils as contacts on personal social-media accounts;
- protect confidential and personal information;

- not post content that could compromise pupils, colleagues or the school; and
- report safeguarding concerns or inappropriate contact promptly.

Official school accounts may only be created or managed with the headteacher's approval. Access will be restricted to authorised staff, account security will be maintained and published content will be checked before posting.

Pupils will be taught about age restrictions, privacy, respectful communication, online reputation and how to report or block harmful contact.

Online conduct outside school may be addressed where it creates a safeguarding risk, affects pupils' welfare or education, or adversely affects the school community.

21. The school website

The headteacher has overall responsibility for ensuring that the school website is accurate, appropriate, accessible and kept up to date.

Only authorised staff may publish or amend content. Before publication, the school will consider:

- safeguarding and data-protection requirements;
- consent for the use of photographs, video or pupil work;
- whether pupils or staff could be identified unnecessarily;
- copyright and licensing;
- accessibility; and
- the accuracy and currency of information.

Personal contact details for pupils or individual members of staff will not be published unless there is a clear, lawful and approved reason.

Website content will be reviewed regularly, and inaccurate or outdated information will be amended or removed promptly.

22. Use of devices

School-owned devices will be securely configured, maintained and used in accordance with the relevant Acceptable Use Agreement.

Users must:

- protect devices from loss, damage and unauthorised access;
- use their own account and keep login details secure;
- install only authorised software or applications;
- store school information using approved systems;
- lock devices when unattended;
- report loss, damage or suspected compromise immediately; and
- return devices when requested or when access is no longer required.

School-owned devices remain subject to the school's filtering, monitoring and security arrangements, including when used away from the school site where technically possible.

Personal devices may only be used for school purposes when authorised and in accordance with the relevant school policy. Personal devices must not be used to photograph, record or store information about pupils unless specifically approved.

Reasonable adjustments may be made for medical, accessibility or SEND-related needs.

23. Remote learning

Remote learning will be delivered through school-approved systems and in accordance with the Remote Education Policy, safeguarding procedures and Staff Code of Conduct.

The school will ensure that:

- appropriate privacy and security settings are used;
- staff use school accounts and maintain professional boundaries;
- pupils and parents understand expectations for behaviour and participation;
- communication and live sessions are appropriate and suitably supervised;
- personal information is not displayed or shared unnecessarily;
- recording only takes place when authorised and for a clear purpose; and
- pupils know how to report concerns or seek help.

Staff will consider pupils who may be more vulnerable or unable to access remote learning safely. Appropriate support or alternative arrangements will be provided where possible.

Safeguarding concerns arising during remote learning will be reported to the DSL without delay. Filtering and monitoring will be applied to school-managed devices used remotely where technically possible.

24. Monitoring and review

The headteacher and DSL will monitor the implementation and effectiveness of this policy using:

- safeguarding and behaviour information;
- filtering and monitoring reports;
- pupil, staff and parent feedback;
- curriculum monitoring;
- staff training records;
- online-safety and cyber-security risk assessments; and
- lessons learned from incidents.

The policy will be reviewed formally at least annually by the headteacher, DSL and governing board.

An earlier review will take place following:

- a serious online-safety incident;
- a significant change to technology or school provision;
- an identified weakness in the school's arrangements; or
- a relevant change to legislation or guidance.

The governing board will approve material changes. Updated requirements will be communicated to staff, pupils and parents where relevant.

Key responsibilities and reporting routes

- Designated safeguarding lead: Amy Hughes, Headteacher
- Deputy designated safeguarding lead(s): Kim Abbott, Assistant Headteacher, Amy Southwick, Assistant Headteacher, Kirsty Niziolek, Business Manager
- SLT lead for filtering and monitoring: Amy Hughes, Headteacher
- Governor responsible for filtering and monitoring: John Webster
- IT support/provider: Roger Fressanges
- Data protection officer: Kirsty Niziolek, Business Manager
- Pupil safeguarding concerns must be recorded using: CPOMS
- Filtering failure or inappropriate content must be reported to: Roger Fressanges
- Suspected cyber-security incidents must be reported to: RPA Cyber Emergency Assistance. By telephone: 0800 368 6378 or by email: RPAresponse@CyberClan.com
- If the DSL is unavailable, staff must contact: [deputy DSL or safeguarding escalation route]
- An immediate risk of serious harm must be reported to the emergency services by calling 999. Staff must then notify the DSL or headteacher as soon as possible.