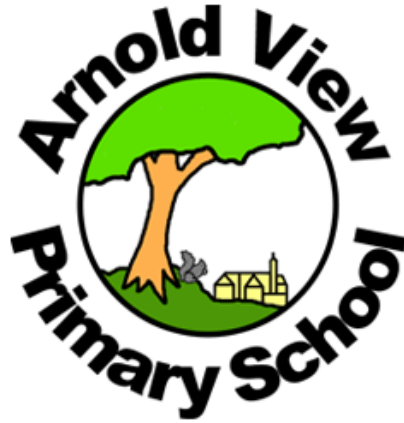




Arnold View Primary School

Online Safety Policy

Policy owner: Designated Safeguarding Lead / Online Safety Lead

Approved by: Governing Body

Date approved: August 2026

Effective from: September 2026

Version: 1.0

Review date: September 2027

1. Introduction

Arnold View Primary School recognises that technology is an integral part of children's lives and has an important role in teaching, learning, communication and school administration.

The school is committed to ensuring that pupils, staff, governors, volunteers, parents, carers and visitors are able to use technology safely, responsibly and positively.

Online safety is an integral part of safeguarding and child protection. It is not solely an IT responsibility. The school recognises that online risks can arise in school, at home and in the wider community, and that online experiences can affect children's safety, mental health, wellbeing, relationships, behaviour and learning.

This policy should be read alongside the school's:

- Safeguarding and Child Protection Policy;
- Behaviour Policy;
- Anti-Bullying Policy;
- Mobile Phone and Personal Devices Policy;
- Data Protection Policy;
- Technical Security Policy;
- Filtering and Monitoring arrangements;
- Artificial Intelligence guidance/policy;
- Acceptable Use Agreements;
- Searching, Screening and Confiscation procedures;
- Staff Code of Conduct;
- Complaints and Whistleblowing procedures.

The policy applies to the use of school technology and school systems both on and away from the school site, and to personal devices when their use is permitted on school premises.

Where online behaviour occurring outside school affects the safety, wellbeing or relationships of pupils or the wider school community, the school will respond in accordance with its safeguarding, behaviour and anti-bullying procedures.

2. Aims

The aims of this policy are to:

1. safeguard children and adults when using technology;
2. provide clear expectations for safe and responsible use of digital technology;
3. ensure that online safety is embedded within the school's safeguarding culture;
4. provide age-appropriate online safety education throughout the school;
5. ensure that staff understand their responsibilities and professional boundaries;
6. provide clear and accessible routes for reporting online safety concerns;
7. ensure that filtering and monitoring are effective and appropriately overseen;
8. promote responsible, ethical and safe use of artificial intelligence;
9. protect personal information and comply with applicable data protection requirements;
10. support parents and carers in helping children develop safe and responsible online behaviours;

11. ensure that incidents are dealt with promptly, proportionately and consistently;
 12. use incidents, monitoring information and pupil feedback to improve practice.
-

3. Scope

This policy applies to:

- all pupils;
- all teaching and support staff;
- the Headteacher and senior leaders;
- the Designated Safeguarding Lead (DSL) and deputies;
- governors;
- volunteers and students;
- contractors and technical support staff;
- parents and carers where they use school systems or platforms;
- visitors and community users who are given access to school technology.

It applies to:

- school-owned computers, tablets and other devices;
 - school networks and internet connections;
 - school email and accounts;
 - cloud services and learning platforms;
 - approved educational applications and websites;
 - school-managed mobile and smart devices;
 - online communication undertaken on behalf of the school;
 - personal devices where their use is permitted on school premises or involves school systems.
-

4. Roles and Responsibilities

4.1 Governing Body

The governing body has strategic oversight of online safety and will:

- ensure that online safety forms part of the school's safeguarding arrangements;
- approve this policy and monitor its effectiveness;
- ensure that staff receive appropriate safeguarding and online safety training;
- understand the school's filtering and monitoring arrangements;
- challenge leaders appropriately regarding the effectiveness of filtering, monitoring and online safety education;
- receive appropriate information about online safety incidents, trends and actions;
- ensure that relevant policies and procedures are reviewed when risks or technology change.

The governing body will nominate a governor to maintain oversight of online safety and filtering and monitoring.

The Online Safety Governor will:

- meet with the DSL and/or Online Safety Lead as appropriate;
- receive appropriate anonymised information about incidents and emerging risks;
- understand the school's filtering and monitoring arrangements;

- contribute to the annual review of filtering and monitoring;
- report relevant findings to the governing body;
- undertake appropriate online safety and cyber-security awareness training.

4.2 Headteacher and Senior Leaders

Senior leaders are responsible for establishing a strong culture of online safety and ensuring that appropriate systems are in place.

They will:

- ensure that the school fulfils its safeguarding responsibilities in relation to online safety;
- ensure that the DSL has sufficient authority, training and support;
- ensure that staff understand their online safety responsibilities;
- ensure that appropriate filtering and monitoring arrangements are in place;
- ensure that concerns and incidents are acted upon appropriately;
- ensure that relevant staff understand the operation and limitations of filtering and monitoring;
- ensure that online safety is reflected in curriculum planning and staff development;
- ensure that serious allegations involving staff or volunteers are dealt with through the appropriate safeguarding and managing-allegations procedures;
- receive regular reports on online safety risks, incidents and emerging themes.

A nominated senior leader will work with the DSL and technical provider to oversee the effectiveness of filtering and monitoring.

5. Designated Safeguarding Lead

The DSL retains lead responsibility for safeguarding, including online safety.

The DSL will:

- maintain appropriate knowledge of online safety risks;
- ensure online safety concerns are recorded and managed through safeguarding procedures;
- provide or arrange appropriate support for pupils affected by online harm;
- liaise with parents/carers and external agencies where appropriate;
- work with senior leaders and technical staff regarding filtering and monitoring;
- participate in the annual review of filtering and monitoring;
- review patterns and trends in online safety incidents;
- ensure that relevant staff understand how to report online safety concerns;
- ensure that pupils with additional needs, vulnerabilities or SEND receive appropriate support;
- ensure that online safety concerns are referred or escalated where necessary.

The DSL will use professional curiosity and will not assume that the absence of a disclosure means that online harm is not occurring.

6. Online Safety Lead

Where the school appoints an Online Safety Lead, that person will support the DSL in the day-to-day development and implementation of online safety.

The Online Safety Lead will:

- support the DSL in maintaining this policy;
- coordinate online safety education;
- support staff training;
- work with curriculum leaders to ensure progression in online safety learning;
- promote pupil voice and participation;
- liaise with technical staff;
- support parent and carer engagement;
- maintain awareness of emerging online risks;
- contribute to the review of incidents and trends.

The DSL remains accountable for safeguarding decisions.

7. Staff Responsibilities

All staff are expected to model safe, respectful and professional online behaviour.

Staff will:

- follow this policy and the school's Acceptable Use Agreement;
- follow the Safeguarding and Child Protection Policy and Staff Code of Conduct;
- maintain appropriate professional boundaries with pupils and families;
- use school-approved digital services and accounts for school business;
- protect passwords and personal information;
- follow data protection requirements;
- supervise pupils appropriately when they are using technology;
- report online safety concerns promptly;
- challenge harmful or inappropriate online behaviour;
- ensure that digital resources are appropriate for pupils;
- teach children how to use technology safely and responsibly;
- respect copyright and intellectual property;
- use only school-approved AI tools for school purposes;
- check AI-generated information before relying upon or sharing it;
- complete required safeguarding, online safety and cyber-security training.

Staff must not use personal email, personal social media accounts or personal messaging services to communicate privately with pupils or establish inappropriate online relationships with pupils or families.

Any exceptional communication arrangement must be authorised by the school and comply with safeguarding and professional conduct requirements.

8. Technical Provider and Technical Staff

The school remains responsible for safeguarding arrangements even where technical services are provided by an external organisation.

The technical provider will support the school by:

- maintaining secure networks and systems;
- managing user access and permissions;
- maintaining appropriate filtering and monitoring;
- providing relevant reports and alerts;
- responding to technical incidents;
- supporting the annual filtering and monitoring review;
- maintaining appropriate security controls, updates and malware protection;
- supporting backup and recovery arrangements;

- advising leaders about technical risks and limitations.

Technical staff will report safeguarding concerns promptly to the DSL or an appropriate senior leader.

Technical monitoring does not replace professional safeguarding judgement.

9. Pupils

Pupils are expected to:

- use technology safely, respectfully and responsibly;
- follow the school's age-appropriate Acceptable Use Agreement;
- treat other people kindly online and offline;
- protect their personal information;
- keep passwords private;
- tell a trusted adult if something online worries, upsets or frightens them;
- report harmful, inappropriate or suspicious online behaviour;
- respect other people's privacy;
- respect copyright and intellectual property;
- use school technology for its intended purpose;
- follow age restrictions and school rules for online services;
- use AI only when permitted and in accordance with school guidance.

Children will be taught that making a mistake online or seeing something inappropriate is not, in itself, a reason to avoid asking for help.

10. Parents and Carers

Parents and carers are important partners in keeping children safe online.

The school will:

- communicate key online safety messages to families;
- provide information about online risks and emerging technologies;
- explain the school's expectations regarding personal devices;
- provide information about the school's online safety curriculum;
- provide appropriate opportunities for parents/carers to access guidance and support;
- signpost families to trusted sources of online safety advice;
- provide clear information about how concerns can be reported;
- communicate relevant changes to school policy.

Parents and carers are encouraged to:

- take an active interest in their child's online experiences;
- establish age-appropriate boundaries;
- use parental controls where appropriate;
- understand the age restrictions applying to services their child uses;
- encourage children to tell them about anything that worries them online;
- report safeguarding concerns to the school where appropriate.

11. Online Safety Education

Online safety education is a core part of the school's safeguarding and curriculum provision.

It will be:

- planned and progressive;

- age-appropriate;
- inclusive;
- responsive to emerging risks;
- connected to children's real experiences;
- reinforced across the curriculum and wider school life.

The school may use recognised resources and frameworks, including Project EVOLVE and Education for a Connected World, alongside appropriate DfE and UK Safer Internet Centre guidance.

Online safety education will address, as appropriate:

- online relationships and friendships;
- kindness and respectful communication;
- cyberbullying;
- privacy and personal information;
- passwords and account security;
- inappropriate content;
- online grooming and exploitation;
- image sharing and consent;
- scams and financial safety;
- gaming and in-game communication;
- social media and age restrictions;
- misinformation and unreliable information;
- digital wellbeing and screen use;
- copyright and intellectual property;
- artificial intelligence;
- online reputation;
- reporting concerns and seeking help.

11.1 EYFS and Key Stage 1

For younger children, teaching will focus on simple, memorable messages such as:

- ask before using technology when necessary;
- tell a trusted adult if something feels wrong;
- be kind online;
- keep personal information private;
- use devices carefully;
- only use websites and applications approved by adults;
- understand that not everything seen online is true or suitable.

11.2 Key Stage 2

As pupils mature, teaching will develop their understanding of:

- online identity and reputation;
- age restrictions;
- online friendships and group communication;
- gaming and chat;
- image sharing;
- scams and manipulation;
- harmful content;

- misinformation;
- privacy and data;
- copyright;
- AI-generated content;
- responsible use of AI;
- reporting, blocking and seeking help.

The school will not rely on technical restrictions alone. Children will be taught the knowledge and skills necessary to make safer decisions.

12. Acceptable Use

The school uses age-appropriate Acceptable Use Agreements for pupils, staff, parents/carers, volunteers and other authorised users.

Acceptable Use Agreements will be:

- explained rather than simply signed;
- reinforced through teaching and reminders;
- reviewed when technology or risks change;
- appropriate to the age and understanding of pupils.

Users must not use school systems to create, access, store, transmit or share material that is illegal, harmful, threatening, discriminatory, abusive or otherwise contrary to school policy.

This includes, but is not limited to:

- child sexual abuse material;
- grooming or exploitation;
- terrorist or extremist material;
- threats of violence;
- hate-related material;
- harassment or stalking;
- illegal drugs or weapons-related activity;
- fraud;
- unauthorised access to systems;
- malware or deliberate disruption;
- phishing or credential theft;
- deliberate attempts to bypass school filtering or security;
- deliberate access to pornography or other inappropriate material;
- bullying or harassment;
- unauthorised sharing of personal information;
- infringement of copyright;
- unauthorised commercial activity using school systems.

The school will distinguish between accidental access, inappropriate behaviour and deliberate or potentially illegal activity, and will respond proportionately.

13. Personal Devices and Mobile Phones

The school operates a mobile-phone-free environment in accordance with its Behaviour Policy and current Department for Education requirements.

Pupils should not have access to mobile phones or other personal smart devices during the school day except where an authorised exception applies.

Exceptions may be made where required for:

- medical reasons;
- safeguarding;
- accessibility;
- SEND;
- another specific need agreed by the school.

Any exception must be clearly authorised and appropriately managed.

The school will have clear procedures for:

- bringing devices onto the premises;
- storage;
- authorised use;
- confiscation where appropriate;
- searching where permitted;
- return of devices;
- managing breaches of the rules.

Staff will model the school's expectations and will use personal devices only where authorised and professionally appropriate.

14. Digital Content, Photography and Recording

The creation and sharing of photographs, videos and audio recordings must comply with:

- safeguarding requirements;
- data protection requirements;
- consent arrangements;
- school procedures;
- professional expectations.

Staff and pupils must not take, store or share images or recordings of other people without appropriate authority.

The school recognises that digital content can be copied, altered, republished or distributed beyond its intended audience.

Particular care will be taken with children's images and personal information.

AI-generated or AI-assisted images and other content will be considered carefully before publication, particularly where real people or children are represented.

15. Artificial Intelligence

The school recognises that artificial intelligence can provide educational and administrative benefits but also introduces safeguarding, privacy, accuracy, bias, copyright and ethical risks.

AI use must be:

- safe;
- age-appropriate;
- purposeful;
- transparent where appropriate;
- subject to human oversight;
- compliant with school data protection requirements.

Staff

Staff may only use AI tools approved by the school for school purposes.

Staff must not enter personal, confidential or sensitive information about pupils, families or colleagues into an AI service unless the school has explicitly approved that use and the appropriate data protection requirements have been satisfied.

Staff remain professionally responsible for any work produced with AI assistance.

AI outputs must be checked for:

- accuracy;
- appropriateness;
- bias;
- safeguarding concerns;
- copyright or intellectual property issues.

AI must not replace professional judgement, particularly when decisions affect pupils, staff or families.

Pupils

Pupils will be taught about AI in an age-appropriate way.

They will learn that:

- AI can make mistakes;
- AI-generated information is not necessarily true;
- AI can reproduce bias;
- personal information should not be entered into AI systems;
- AI should not be used to cheat or misrepresent work;
- other people's work and images must be respected;
- harmful or inappropriate AI-generated content should be reported.

AI may only be used by pupils where it has been specifically permitted and supervised by the school.

16. Filtering and Monitoring

The school maintains filtering and monitoring arrangements designed to reduce the risk of children accessing illegal, inappropriate or harmful online content.

Filtering and monitoring will be:

- safeguarding-led;
- proportionate;
- regularly reviewed;
- appropriate to the age and role of the user;
- supported by clear reporting arrangements.

The school recognises that no filtering or monitoring system can identify every risk.

Filtering and monitoring therefore supports, but does not replace:

- supervision;
- professional curiosity;
- education;
- reporting;
- safeguarding judgement.

All relevant school-owned devices and internet connections will be subject to appropriate controls.

Where personal devices are authorised to use school systems, the school will make clear what monitoring or filtering applies.

16.1 Annual Review

The effectiveness of filtering and monitoring will be reviewed at least annually and following significant changes or incidents.

The review will involve appropriate representatives from:

- senior leadership;
- safeguarding;
- technical support;
- governance.

The review will consider:

- whether filtering is operating as intended;
- whether inappropriate and illegal content is appropriately blocked;
- whether monitoring identifies relevant concerns;
- whether alerts are being acted upon appropriately;
- whether all relevant devices and locations are covered;
- whether staff understand reporting procedures;
- whether technical limitations are understood;
- whether changes are required.

The school will keep a record of the review, findings and actions.

17. Technical and Cyber Security

The school will take reasonable and proportionate measures to protect its systems and information.

These include:

- appropriate authentication and access controls;
- secure configuration;
- software and security updates;
- malware protection;
- appropriate backups;
- secure handling of data;
- controlled user permissions;
- incident response arrangements;
- staff awareness training.

Staff and pupils will be encouraged to report:

- suspicious emails;
- unexpected login requests;
- lost or stolen devices;
- suspected malware;
- compromised passwords;
- unusual system behaviour;
- suspected data breaches.

The school will respond to cyber-security incidents in accordance with its technical security and incident-response procedures.

18. Data Protection

The school will comply with applicable data protection legislation and its own Data Protection Policy.

Personal data will be:

- processed lawfully, fairly and transparently;

- collected only where appropriate;
- stored securely;
- shared appropriately;
- disposed of securely.

The school will maintain appropriate arrangements for:

- data protection training;
- data breaches;
- Data Protection Impact Assessments;
- privacy notices;
- Subject Access Requests;
- Freedom of Information requests;
- procurement and review of digital services.

Particular care will be taken when using online services involving children and when considering the processing of children's personal information.

The school's Data Protection Officer will advise on data protection matters where required.

19. Reporting Online Safety Concerns

The school wants all members of its community to feel confident reporting concerns.

Pupils can report concerns by:

- telling a trusted adult;
- speaking to their class teacher;
- speaking to the DSL or a deputy;
- using an age-appropriate school reporting mechanism where provided.

Staff must report safeguarding or online safety concerns to the DSL or deputy without delay.

Parents and carers can raise concerns through the school's established safeguarding or communication routes.

Concerns may include:

- cyberbullying;
- harmful or inappropriate content;
- grooming;
- exploitation;
- sexual harassment;
- image sharing;
- threats;
- discrimination;
- hate-related behaviour;
- scams;
- suspected illegal activity;
- concerning contact from another person;
- harmful use of AI.

Children will be reassured that reporting a concern is the right thing to do.

20. Responding to Incidents

All online safety incidents will be considered on the basis of:

- the nature and seriousness of the concern;

- the age and vulnerability of the child;
- whether there is an immediate safeguarding risk;
- whether illegal activity may have occurred;
- whether the behaviour is part of a wider pattern;
- the impact on other members of the school community.

The DSL will determine whether an incident should be managed through:

- normal classroom or behaviour procedures;
- safeguarding procedures;
- the anti-bullying process;
- technical intervention;
- parental involvement;
- external agency referral;
- police involvement.

Where there is a safeguarding concern, staff must not attempt to conduct their own investigation.

Evidence should be preserved where appropriate and staff should follow the DSL's instructions and the school's incident procedures.

21. Devices and Evidence

Where a device needs to be checked following an incident, this will only be undertaken in accordance with the school's Behaviour Policy, searching procedures and applicable statutory guidance.

Searching will be carried out only by appropriately authorised staff and will be proportionate to the concern.

Where there may be illegal content or serious safeguarding concerns, the school will seek appropriate advice and will not undertake inappropriate investigation of potentially criminal evidence.

Technical staff may assist with the preservation of evidence but safeguarding decisions remain the responsibility of school leaders.

22. External Agencies

Where necessary, the school will work with appropriate external agencies, which may include:

- the Local Authority;
- the Local Safeguarding Partnership;
- the Local Authority Designated Officer;
- police;
- CEOP;
- relevant safeguarding professionals;
- appropriate specialist online safety organisations.

Referrals will be made in accordance with the school's safeguarding procedures and local arrangements.

23. Online Behaviour Outside School

The school recognises that pupils may experience online bullying, harmful content or inappropriate contact outside school.

Where such behaviour affects the safety, wellbeing, relationships or education of pupils or the wider school community, the school may need to become involved.

Any response will be proportionate and will follow the school's safeguarding, behaviour and anti-bullying procedures.

Parents and carers will be informed where appropriate.

24. Staff Training

All staff and volunteers will receive safeguarding training that includes online safety.

Training will address, as appropriate:

- current online risks;
- reporting procedures;
- filtering and monitoring;
- professional boundaries;
- cyber security;
- data protection;
- mobile-device expectations;
- AI;
- online bullying;
- harmful sexual behaviour and image sharing;
- children's vulnerabilities;
- appropriate use of technology in teaching.

Training will be refreshed regularly and whenever significant changes in risk, technology or guidance require an update.

The DSL and Online Safety Lead will maintain their knowledge through appropriate professional development.

25. Governor Training

Governors will receive appropriate online safety awareness and safeguarding information.

The governor with responsibility for online safety will receive additional information or training concerning:

- filtering and monitoring;
- cyber security;
- safeguarding risks;
- online safety education;
- the effectiveness of the school's arrangements.

26. Parent and Carer Engagement

The school will support families through:

- newsletters;
- information on the school website;
- parent meetings or workshops where appropriate;
- curriculum information;
- signposting to trusted resources;
- information about emerging online risks;
- guidance on reporting concerns.

The school may signpost families to organisations such as:

- UK Safer Internet Centre;
- Childnet;
- National College;
- Internet Matters;
- SWGfL;
- CEOP.

27. Public Online Communications

Only authorised staff may publish content on official school online accounts.

Public communications must:

- be appropriate;
- protect children's privacy;
- comply with data protection requirements;
- reflect the school's values;
- be accurate;
- avoid unnecessary safeguarding risks.

Images and information relating to pupils will be shared in accordance with the school's consent and data protection arrangements.

AI-assisted content will be checked by an authorised member of staff before publication.

The school will take reasonable steps to reduce risks associated with publicly available images being copied, altered or misused.

28. Monitoring, Evaluation and Review

The effectiveness of this policy will be monitored through evidence including:

- online safety incident records;
- safeguarding records;
- behaviour and bullying records;
- filtering and monitoring reports;
- staff feedback;
- pupil voice;
- parent/carers feedback;
- staff training records;
- curriculum review;
- annual filtering and monitoring review.

The school will look for patterns and emerging risks rather than considering incidents in isolation.

Findings will be used to:

- improve policy and procedures;
- update training;
- adapt curriculum provision;
- improve technical controls;
- support individual pupils;
- communicate relevant information to parents and carers;
- inform governors.

This policy will be reviewed at least annually and sooner where there are significant changes to technology, legislation, statutory guidance or identified safeguarding risks.

Related Documents

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Mobile Phone and Personal Devices Policy
- Staff Code of Conduct
- Staff Acceptable Use Agreement
- Pupil Acceptable Use Agreements
- Parent/Carer Acceptable Use Agreement
- Filtering and Monitoring Policy
- Technical Security Policy
- Cyber Security Policy
- Data Protection Policy
- Artificial Intelligence Policy/Guidance
- Searching, Screening and Confiscation Procedure
- Online Safety Incident Recording Procedure
- Public Online Communications Policy

Appendix A: Staff Acceptable Use Agreement (AUA)

Arnold View Primary School

Staff Acceptable Use of School IT Systems and the Internet

This agreement applies to all employees, governors, volunteers, students, agency staff, contractors and any other individual granted access to Arnold View Primary School's ICT systems, devices, networks, internet connection, email services, cloud platforms and digital resources. It supports the requirements of the school's Online Safety Policy.

I understand that the school's IT systems are provided primarily to support teaching, learning, safeguarding and the efficient operation of the school. I agree to use all school technology responsibly, professionally and in accordance with safeguarding, data protection and professional conduct requirements.

I will:

- Use school IT systems for legitimate educational and professional purposes.
- Follow the school's Online Safety Policy, Safeguarding and Child Protection Policy, Staff Code of Conduct, Data Protection Policy and all related procedures.
- Use only my authorised username and password and keep passwords secure and confidential.
- Lock or log out of devices when unattended.
- Report any suspected security breach, cyber incident, phishing attempt, malware infection or loss of data immediately.
- Use only approved software, applications and online services for school business.
- Handle personal data in accordance with UK GDPR, the Data Protection Act 2018 and school procedures.
- Ensure that confidential information is not accessed, shared or discussed inappropriately.
- Maintain professional boundaries with pupils, parents and carers at all times.
- Use school email accounts and approved communication platforms for school-related communication.
- Report immediately to the Designated Safeguarding Lead (DSL) any online safety, safeguarding or welfare concern involving a pupil.
- Check the accuracy and suitability of information before sharing it with pupils, parents or colleagues.
- Use school-approved Artificial Intelligence (AI) tools only where authorised.
- Carefully review and verify all AI-generated content before use.
- Complete required safeguarding, online safety, cyber security and data protection training.
- Respect copyright, licensing agreements and intellectual property rights.

- Use technology in a manner that protects the reputation of the school and its community.

I will not:

- Share passwords or permit another person to use my login credentials.
- Attempt to bypass, disable or interfere with filtering, monitoring or security systems.
- Access, create, store, download or distribute material that is illegal, harmful, offensive, extremist, discriminatory, sexually explicit or otherwise inappropriate.
- Use school systems to harass, intimidate, bully or victimise any individual.
- Use personal email accounts, personal messaging services or personal social media accounts to communicate privately with pupils.
- Establish inappropriate online relationships with pupils or former pupils.
- Install software, applications or browser extensions without authorisation.
- Connect unauthorised devices to the school's network.
- Access another user's files, folders or accounts without permission.
- Share personal, confidential or sensitive information with AI tools unless specifically authorised by the school and compliant with data protection requirements.
- Download or copy school information to personal devices without authorisation.
- Use school IT systems for personal commercial activities or political campaigning.
- Deliberately access inappropriate websites or online content.
- Photograph, film or record pupils using personal devices unless expressly authorised in accordance with school procedures.

Monitoring

I understand that:

- The school has a duty to safeguard children and protect its systems.
- Use of school ICT systems, devices, internet access and communications may be monitored, recorded and reviewed for safeguarding, security, operational and legal purposes.
- Monitoring is carried out in accordance with relevant legislation and school policies.
- The school may investigate misuse of its systems and take appropriate action where necessary.

Artificial Intelligence

I understand that:

- AI-generated content may be inaccurate, biased or incomplete.
- Professional judgement remains my responsibility at all times.

- AI must never replace safeguarding decision-making or professional assessment.
- Confidential pupil, staff or family information must not be entered into AI systems unless the school has explicitly approved such use.

Breaches of this Agreement

I understand that any breach of this agreement may result in:

- Withdrawal of IT access;
- Internal investigation;
- Disciplinary action;
- Referral to external agencies;
- Referral to the police where appropriate.

Declaration

I have read, understood and agree to comply with the Arnold View Primary School Staff Acceptable Use Agreement, Online Safety Policy and associated policies.

Name: _____

Role: _____

Signature: _____

Date: _____