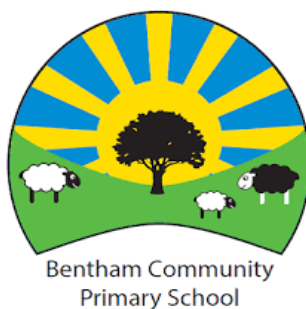




Bentham Community Primary School

Workforce Digital Technology, Artificial Intelligence (AI) and Acceptable Use Policy

Date approved: September 2026

Review date: September 2027

Headteacher (SIRO): Mr Richard Wright

Chair of Governors: Mr Chris Hawkins

Responsible Committee: Finance, Resources and Compliance Committee

Digital Innovation Statement

Bentham Community Primary School recognises that digital technology and Artificial Intelligence (AI) are increasingly important tools in education.

The school is committed to embracing innovation where it improves teaching, learning and operational efficiency, whilst ensuring that all technology is used safely, ethically, securely and in accordance with safeguarding, data protection and professional standards.

Artificial Intelligence should enhance professional practice rather than replace professional judgement.

This policy therefore provides the school's framework for the responsible use of digital technology, AI and online services by all members of the workforce.

Purpose of this Policy

This policy sets out the expectations for the safe, secure, professional and responsible use of digital technologies by all members of the workforce at Bentham Community Primary School.

Technology plays a vital role in teaching, learning, communication, safeguarding and the day-to-day operation of the school. Used effectively, digital technologies enhance education, improve efficiency and strengthen collaboration. However, they also bring responsibilities and risks that require all staff to exercise professional judgement and maintain the highest standards of conduct.

This policy provides a clear framework for the appropriate use of school technology, digital communication, cloud-based services, Artificial Intelligence (AI), personal devices and online platforms. It supports the school's commitment to safeguarding children, protecting personal information, maintaining cyber security and promoting public confidence in the school.

This policy supports the school's responsibilities under **Keeping Children Safe in Education (current edition)**, recognising that safeguarding extends to the safe and responsible use of digital technologies and Artificial Intelligence.

It also takes into account important legal frameworks that include:

- UK GDPR
- Data Protection Act 2018
- Freedom of Information Act 2000
- Keeping Children Safe in Education (current edition)
- Prevent Duty Guidance
- Equality Act 2010
- Department for Education cyber security guidance
- Department for Education guidance on the use of AI in education (where applicable)

This policy should also be read alongside the school's:

- Child Protection and Safeguarding Policy
- Data Protection Policy
- Information Security Policy
- Records Management Policy
- Online Safety Policy
- Staff Code of Conduct
- Disciplinary Policy
- Remote Working Guidance
- Social Media Guidance
- ICT Disaster Recovery and Business Continuity Plans.

Our Digital Vision

At Bentham Community Primary School we believe that digital technology should enable children and adults to learn, communicate and work safely, confidently and responsibly.

Technology should enhance education—not replace professional expertise.

We are committed to creating a positive digital culture where:

- technology improves teaching and learning
- staff use digital systems confidently and responsibly
- children are safeguarded online
- confidential information is protected
- innovation is encouraged within appropriate professional boundaries
- Artificial Intelligence supports professional practice responsibly
- cyber security is everyone's responsibility.

Digital responsibility is an essential part of professional practice and reflects our wider school values.

Scope of this Policy

This policy applies to everyone working for or on behalf of Bentham Community Primary School, including:

- employees
- governors
- volunteers
- trainee teachers
- agency staff
- contractors
- consultants
- peripatetic staff
- visitors with authorised access to school systems.

The policy applies whenever school digital systems, networks, devices or information are accessed, whether:

- on school premises
- working remotely
- at home
- whilst travelling
- on school visits
- using school-owned equipment
- using authorised personal devices.

The expectations within this policy apply equally regardless of the device or location used.

Our Digital Expectations

Every member of staff is expected to:

- act professionally at all times
- safeguard children in both physical and digital environments
- protect confidential information
- maintain secure digital practices
- model positive online behaviour
- use technology ethically and responsibly
- report cyber security concerns immediately
- comply with data protection legislation
- use Artificial Intelligence responsibly
- protect the reputation of the school
- continually develop their digital knowledge and skills.

Digital professionalism is everyone's responsibility.

Professional Responsibilities

Every member of staff is personally responsible for their use of digital technology.

Professional standards that apply within school also apply online.

Staff are expected to demonstrate the same levels of professionalism when using email, social media, messaging services, online meetings and digital platforms as they would during face-to-face interactions.

Staff must always consider whether their digital behaviour:

- protects children
- maintains confidentiality
- reflects the school's values
- complies with legislation
- protects public confidence in the school.

Digital communication should always be respectful, professional, accurate and appropriate.

Professional Digital Conduct

Technology should be used to support effective education and positive working relationships.

All staff are expected to:

- communicate respectfully
- maintain appropriate professional boundaries
- use approved communication systems
- consider how written communication may be interpreted by others
- maintain confidentiality
- avoid language that could be misunderstood
- use emojis, informal messaging and abbreviations appropriately
- avoid sarcasm or humour that could be misinterpreted
- challenge inappropriate digital behaviour where appropriate.

Professional conduct applies equally to:

- email
- Microsoft Teams
- Google Workspace
- video conferencing
- messaging platforms
- collaborative working tools
- AI systems
- social media.

Digital Safeguarding

Safeguarding remains the school's highest priority.

Digital technology should always support, and never compromise, the safety and wellbeing of children.

Members of staff must:

- use only approved school communication systems when communicating with pupils
- never use personal social media accounts to communicate with pupils
- never exchange personal telephone numbers unless authorised through school procedures
- maintain appropriate professional boundaries at all times
- immediately report any safeguarding concern arising from digital communication
- follow the school's Child Protection and Safeguarding Policy where concerns arise.

Staff should remain alert to online risks including:

- cyberbullying
- online grooming
- inappropriate content

- radicalisation
 - online exploitation
 - misinformation
 - malicious communication
 - AI-generated images or content intended to exploit or harm children.
-

Artificial Intelligence (AI)

The school recognises that Artificial Intelligence is becoming an increasingly valuable tool within education and the school will have regard to relevant Department for Education guidance regarding the safe, ethical and effective use of Artificial Intelligence in education as this continues to develop.

Used responsibly, AI can improve efficiency, reduce workload and support high-quality teaching and learning.

Artificial Intelligence should enhance professional practice, reduce unnecessary workload and support better outcomes for pupils, but it must never replace professional judgement or accountability

Members of staff may use approved AI systems to support professional activities such as:

- lesson planning
- curriculum development
- drafting reports and letters
- creating teaching resources
- generating quizzes and revision materials
- administrative tasks
- summarising non-confidential documents
- professional research
- improving accessibility of learning materials.

Staff remain fully responsible for everything they produce using AI.

Principles for Responsible AI Use

All use of Artificial Intelligence must be guided by the following principles.

Professional Accountability

Staff remain accountable for all decisions, communications and materials produced using AI.

AI must support professional judgement rather than replace it.

Confidentiality

Personally identifiable information relating to pupils, parents, staff or governors must never be entered into publicly available AI systems.

Confidential school information must only be processed using approved systems authorised by the school.

Accuracy

AI systems can produce inaccurate or misleading information.

All AI-generated content must therefore be checked carefully before being:

- shared
 - published
 - emailed
 - presented
 - used for teaching
 - incorporated into reports.
-

Safeguarding

Staff must ensure that AI-generated content is appropriate for children and free from:

- harmful stereotypes
 - inappropriate bias
 - offensive language
 - safeguarding concerns
 - misinformation
 - discriminatory content.
-

Copyright and Intellectual Property

Staff must ensure that AI-generated resources respect copyright, licensing requirements and intellectual property rights.

AI Literacy

The school recognises that responsible use of Artificial Intelligence requires staff to develop appropriate knowledge and understanding. Staff will be supported to:

- understand the capabilities and limitations of AI
 - identify inaccurate or biased outputs
 - use AI ethically and responsibly
 - apply professional judgement when using AI to support their work.
-

Emerging Technology

The school recognises that emerging technologies including Artificial Intelligence, machine learning, wearable technology, extended reality and future digital platforms may present new opportunities and risks. New technologies will be evaluated before adoption to ensure they support education safely, ethically and securely

Information Governance

All members of staff are responsible for protecting the confidentiality, integrity and availability of school information.

Information must always be:

- accessed lawfully
- shared appropriately
- stored securely
- retained in accordance with school procedures
- disposed of securely.

Staff must comply with:

- UK GDPR
- Data Protection Act 2018
- Freedom of Information Act 2000
- school information governance policies.

Protecting personal information is a professional responsibility and forms part of every employee's role.

Equality, Inclusion and Accessibility

Digital technology should improve inclusion and remove barriers to participation.

The school is committed to ensuring technology supports:

- accessibility
- equality of opportunity
- reasonable adjustments
- inclusive communication
- assistive technologies
- equitable access to learning.

Staff should consider the needs of all users when creating digital resources or communicating electronically.

Roles and Responsibilities

Governing Board

The Governing Board provides strategic oversight of information governance, cyber security and digital safeguarding.

Governors will:

- ensure statutory responsibilities are fulfilled
 - monitor cyber security risks
 - oversee information governance arrangements
 - receive assurance regarding digital safeguarding
 - monitor implementation of this policy
 - ensure appropriate resources are available.
-

Headteacher (Senior Information Risk Owner)

The Headteacher is responsible for the strategic management of digital systems and information risk.

The Headteacher will:

- promote a positive digital culture
- ensure compliance with legislation
- oversee information governance
- manage cyber security risks
- approve the use of emerging technologies
- authorise AI systems where appropriate

- ensure appropriate staff training
 - investigate serious breaches of this policy.
-

Every Member of Staff

Every member of staff is responsible for:

- complying with this policy
 - protecting school information
 - safeguarding children online
 - maintaining professional standards
 - reporting cyber security concerns
 - using technology responsibly
 - participating in mandatory digital safety training.
-

Core Principle

Technology is a powerful tool for education.

Its value depends upon the professionalism, integrity and judgement of those who use it.

Every member of the workforce shares responsibility for ensuring that digital technology is used safely, ethically, securely and in ways that support the education, wellbeing and safeguarding of every child.

Using Digital Technology Safely and Responsibly

Digital Communication

Effective communication is fundamental to the safe and efficient operation of the school.

Digital communication should always be professional, respectful and appropriate to the recipient.

Staff should remember that written communication can easily be misunderstood and should therefore communicate clearly, courteously and professionally at all times.

All digital communications may become subject to disclosure under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, Freedom of Information legislation or legal proceedings.

Staff should therefore always write communications with the expectation that they may be read by others.

Email

School email accounts are provided for professional purposes.

School email remains the primary method of formal communication within the organisation and with external agencies.

Staff are expected to:

- use their school email account for all school business
- maintain a professional tone
- proofread emails before sending
- consider whether email is the most appropriate form of communication
- protect confidential information
- use secure methods when sending sensitive information
- ensure recipients are correct before sending emails
- avoid unnecessary use of "Reply All"
- report suspicious emails immediately.

Email should never be used:

- to criticise colleagues
- to express personal grievances
- to discuss confidential matters unnecessarily
- to communicate with pupils using personal email accounts
- to circulate offensive or discriminatory material
- for commercial or political purposes.

Limited personal use of school email may be acceptable provided that it:

- is occasional
 - does not interfere with work
 - complies with this policy
 - does not compromise school systems.
-

Microsoft 365 and Cloud Services

Bentham Community Primary School uses Microsoft 365 and other approved cloud-based systems to support teaching, administration and collaboration.

Staff should:

- access only information required for their role
- ensure documents are stored within approved locations
- avoid creating unnecessary duplicate files
- share documents securely
- check permissions before sharing files
- use version control where appropriate
- log out when using shared devices.

School information should remain within approved cloud systems wherever possible.

Downloading confidential information onto personal devices should be avoided unless specifically authorised.

Artificial Intelligence (AI)

Artificial Intelligence is becoming an increasingly valuable professional tool within education.

The school encourages responsible innovation whilst recognising that AI presents new ethical, safeguarding and information governance challenges.

Staff may use approved AI tools to assist with:

- lesson planning
- curriculum design
- resource creation
- administrative tasks
- drafting letters
- report writing
- creating knowledge organisers
- generating quizzes
- summarising lengthy documents
- accessibility adaptations
- translation support
- professional research.

AI should support professional practice rather than replace professional expertise.

Prohibited AI Use

Staff must never:

- upload confidential school information into publicly available AI systems
- upload personal information relating to pupils, parents or staff

- rely solely upon AI-generated information without checking accuracy
- use AI to produce safeguarding decisions
- use AI to write statutory reports without careful review
- create misleading or fabricated information
- use AI to impersonate another person
- use AI-generated images or videos in ways that could cause harm or misrepresentation.

Professional accountability always remains with the member of staff.

Checking AI Output

Before using AI-generated content, staff must consider:

- Is it accurate?
- Is it factually correct?
- Is it age appropriate?
- Is it inclusive?
- Does it contain bias?
- Does it meet safeguarding expectations?
- Is it appropriate for our curriculum?
- Does it comply with copyright requirements?

No AI-generated content should be used without professional review.

Internet Use

The internet supports learning, communication and professional development.

Staff should use the internet responsibly and professionally.

Internet use should:

- support school business
- promote professional learning
- contribute to teaching and learning
- maintain cyber security
- comply with safeguarding expectations.

Staff should not:

- access inappropriate material
- download unauthorised software
- stream unnecessary media during working hours

- use gambling websites
- visit websites likely to compromise network security
- access offensive, discriminatory or illegal material.

Limited personal browsing during breaks may be acceptable provided it does not interfere with work or compromise school systems.

Cyber Security

Cyber security is everyone's responsibility.

Every member of staff plays an important role in protecting the school from cyber threats.

Staff must:

- remain vigilant
- report suspicious activity immediately
- protect passwords
- maintain secure devices
- complete mandatory cyber security training
- follow school security procedures.

Cyber attacks against schools continue to increase and vigilance is essential.

Passwords and Authentication

Strong passwords remain one of the most effective cyber security controls.

Staff must:

- use strong, unique passwords
- never share passwords
- never record passwords where others may access them
- change passwords immediately if compromise is suspected
- use password managers where approved.

Where Multi-Factor Authentication (MFA) is provided it must always be enabled.

Staff must never approve an authentication request they have not initiated themselves.

Phishing and Cyber Threats

Cyber criminals increasingly target schools through phishing, malicious emails and fraudulent websites.

Staff should always:

- verify unexpected requests
- be cautious of urgent payment requests
- check email addresses carefully
- avoid clicking suspicious links
- avoid opening unexpected attachments
- report suspected phishing immediately.

If uncertain, staff should seek advice before responding.

It is always preferable to report a false alarm than ignore a genuine cyber attack.

Mobile Devices

School-issued mobile devices should be used primarily for school business.

Personal mobile phones should not interfere with professional responsibilities.

Staff must:

- secure devices with passwords or biometrics
- prevent unauthorised access
- report loss immediately
- avoid storing confidential information unnecessarily
- use approved applications.

Where photographs or videos of pupils are required, only school-approved devices should be used unless specifically authorised.

Personal Devices (Bring Your Own Device)

The school recognises that some staff may access school systems using authorised personal devices.

Where personal devices are used, staff must ensure:

- authorisation from the headteacher
- the device is password protected
- operating systems remain updated
- anti-virus software is maintained where appropriate

- automatic security updates are enabled
- devices are not shared whilst logged into school systems
- school information remains within approved cloud systems
- confidential documents are not downloaded unnecessarily.

School information must never be stored permanently on personal devices.

Remote and Hybrid Working

Remote working should maintain the same professional standards expected within school.

When working remotely staff must:

- protect confidential conversations
- prevent family members accessing school information
- lock screens when away from devices
- avoid working in public areas where confidential information may be overlooked
- use secure internet connections
- avoid public Wi-Fi wherever possible.

Printed confidential documents should only be taken off site where absolutely necessary and should be stored and disposed of securely.

Video Conferencing

Video conferencing supports communication, training and collaborative working.

Staff should:

- use approved platforms
- ensure backgrounds are professional
- maintain confidentiality
- dress appropriately
- ensure meetings cannot be overheard where confidential matters are discussed.

Meetings should only be recorded where there is a legitimate business reason and appropriate authorisation.

Participants should be informed before any recording takes place.

Social Media

The school recognises that social media provides valuable opportunities for communication and community engagement.

Staff must remember that public confidence in the school can be affected by online behaviour.

Staff should:

- maintain professional standards
- protect confidentiality
- avoid commenting on pupils or families
- avoid discussing internal school matters publicly
- maintain respectful communication
- consider their digital footprint.

Staff must never:

- communicate with pupils through personal social media accounts
- publish confidential information
- post material that could damage the reputation of the school
- engage in online arguments whilst identifying themselves as members of staff.

Use of Personal Messaging Applications

Personal messaging platforms, including WhatsApp, Facebook Messenger, Signal and similar applications, must not normally be used for communicating with pupils or sharing confidential school information.

Where messaging applications are used for legitimate staff communication:

- participation should be voluntary
- professional standards continue to apply
- confidential information must not be shared
- safeguarding concerns must always be reported through official school procedures.

Digital Records and Information

School information is a valuable organisational asset.

Staff must ensure that information is:

- accurate
- appropriately classified
- securely stored

- retained according to school procedures
- deleted only in accordance with records management requirements.

Staff should avoid creating duplicate records unnecessarily.

Digital Wellbeing

The school recognises that healthy use of digital technology contributes to staff wellbeing.

Staff are encouraged to:

- maintain appropriate boundaries between work and personal life
 - manage digital workloads responsibly
 - use technology efficiently rather than excessively
 - support colleagues in developing healthy digital working practices.
-

Reporting Concerns

All members of staff have a responsibility to report concerns relating to:

- suspected cyber attacks
- phishing attempts
- lost devices
- accidental disclosure of information
- inappropriate use of technology
- safeguarding concerns arising online
- suspected misuse of Artificial Intelligence
- security weaknesses.

Concerns should be reported immediately to the Headteacher, SIRO or appropriate member of the leadership team.

Prompt reporting significantly reduces the impact of cyber incidents and data breaches.

Governance, Monitoring and Accountability

Monitoring Compliance

Bentham Community Primary School is committed to maintaining a secure, safe and professionally responsible digital environment.

Compliance with this policy is monitored to:

- protect pupils and staff
- safeguard confidential information
- reduce cyber security risks
- ensure compliance with legislation
- support effective use of technology
- maintain public confidence in the school.

Monitoring arrangements are proportionate, transparent and undertaken only where there is a legitimate business, safeguarding or legal reason.

The school reserves the right to monitor the use of its digital systems where appropriate and in accordance with relevant legislation.

This may include:

- email activity
- internet usage
- cloud-based systems
- file access
- audit logs
- user accounts
- system security alerts
- device management information.

Monitoring is undertaken in accordance with:

- UK GDPR
- Data Protection Act 2018
- Investigatory Powers legislation where applicable
- Human Rights Act 1998
- school Information Governance policies.

Reporting Security Incidents

Every member of staff has a responsibility to report any actual or suspected information security incident immediately.

Examples include:

- suspicious emails
- phishing attempts
- malware
- ransomware
- lost or stolen devices
- accidental disclosure of information

- unauthorised access
- inappropriate use of school systems
- suspected cyber attacks
- misuse of Artificial Intelligence
- unauthorised sharing of confidential information.

Prompt reporting enables the school to reduce potential harm and fulfil any statutory reporting duties.

Staff should never attempt to investigate serious cyber incidents themselves.

Personal Data Breaches

A personal data breach is any incident which results in the accidental or unlawful:

- destruction
- loss
- alteration
- unauthorised disclosure
- unauthorised access

to personal information.

Examples include:

- sending information to the wrong recipient
- losing paper records
- losing laptops or mobile devices
- uploading confidential information to an unauthorised AI platform
- sharing documents incorrectly
- accidental publication of confidential information.

Any suspected breach must be reported immediately to the Headteacher (Senior Information Risk Owner).

The school will investigate all reported breaches and, where required, notify the Information Commissioner's Office (ICO) within the statutory timescales.

Artificial Intelligence Incident Reporting

The school recognises that emerging technologies introduce new risks.

Staff must immediately report concerns relating to:

- confidential information entered into AI systems
- inaccurate AI-generated content that has been shared
- AI-generated safeguarding concerns
- deepfake images or videos involving members of the school community
- misuse of AI to impersonate staff or pupils
- inappropriate AI-generated learning materials.

The school will investigate all reported concerns and take appropriate action.

Roles and Responsibilities

Governing Board

The Governing Board has strategic responsibility for ensuring effective digital governance across the school.

Governors will:

- approve this policy
- monitor compliance
- oversee information governance
- receive assurance regarding cyber security
- monitor digital safeguarding
- review significant cyber incidents
- ensure sufficient investment in digital infrastructure
- monitor staff training
- challenge leaders regarding digital risks
- ensure this policy remains effective.

The Governing Board recognises that effective digital governance forms an important part of safeguarding and school improvement.

Finance, Resources and Compliance Committee

The Finance, Resources and Compliance Committee provides strategic oversight of:

- information governance
- cyber security
- digital infrastructure
- business continuity
- disaster recovery
- digital resilience
- compliance with statutory responsibilities.

The Committee receives regular assurance regarding cyber security and information governance arrangements.

Headteacher (Senior Information Risk Owner)

The Headteacher, as Senior Information Risk Owner (SIRO), has overall responsibility for managing digital and information risks.

The Headteacher will:

- promote a positive digital culture
 - ensure compliance with legislation
 - oversee information governance
 - approve digital systems
 - authorise AI systems where appropriate
 - investigate serious breaches
 - ensure staff training is provided
 - oversee cyber security arrangements
 - report significant incidents to governors where appropriate.
-

Senior Leadership Team

The Senior Leadership Team will:

- model professional digital behaviour
 - support implementation of this policy
 - monitor emerging digital risks
 - support staff development
 - oversee safeguarding relating to technology
 - evaluate new technologies before implementation
 - ensure appropriate risk assessments are completed.
-

All Members of Staff

Every member of staff is responsible for:

- complying with this policy
- maintaining professional standards
- protecting confidential information
- safeguarding children online
- maintaining secure passwords
- reporting incidents immediately

- completing mandatory training
- using AI responsibly
- protecting the school's reputation.

Professional responsibility cannot be delegated.

Professional Development

Technology continues to evolve rapidly.

The school is committed to ensuring that all staff remain confident, competent and informed.

Annual training will include:

- cyber security awareness
- phishing awareness
- safeguarding and online safety
- information governance
- UK GDPR
- password security
- Artificial Intelligence
- responsible digital communication
- emerging technologies
- updates to legislation and national guidance.

Additional training will be provided where new systems or technologies are introduced.

Acceptable Use

Examples of acceptable use include:

- using approved school systems
- maintaining secure passwords
- using Multi-Factor Authentication
- protecting confidential information
- communicating professionally
- using AI responsibly
- reporting cyber incidents promptly
- completing mandatory training
- using technology to improve teaching and learning
- supporting colleagues to work safely online.

Unacceptable Use

Examples of unacceptable use include:

- sharing passwords
- downloading confidential information onto unauthorised devices
- entering confidential information into unauthorised AI systems
- communicating with pupils through personal social media accounts
- deliberately bypassing security controls
- accessing inappropriate websites
- using school systems for illegal activity
- sharing confidential information without authorisation
- installing unauthorised software
- using technology to bully, harass or discriminate
- creating or sharing inappropriate AI-generated content
- damaging the reputation of the school through inappropriate online behaviour.

This list is not exhaustive.

Failure to Comply

Failure to comply with this policy may result in:

- withdrawal of access to digital systems
- additional training
- management action
- disciplinary procedures
- referral to external agencies where appropriate
- reporting to regulatory bodies where legally required.

Serious misuse of school systems may constitute gross misconduct.

Some breaches may also amount to criminal offences under legislation including:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Fraud Act 2006.

Equality, Inclusion and Accessibility

The school is committed to ensuring that digital technology promotes inclusion rather than creating barriers.

Digital systems should:

- support accessibility
- enable reasonable adjustments
- promote equality of opportunity
- support assistive technologies
- improve participation
- remove unnecessary barriers to learning and employment.

Staff are expected to consider accessibility whenever creating digital resources or communicating electronically.

Policy Review

This policy will be reviewed annually or sooner if required due to:

- changes in legislation
- updates to national guidance
- significant cyber security developments
- emerging technologies
- Artificial Intelligence developments
- information governance requirements
- recommendations arising from incidents
- changes to school systems.

The Governing Board will receive assurance that the policy remains effective and reflects current professional expectations.

Workforce Declaration

All members of the workforce are required to:

- read this policy
- understand their responsibilities
- comply with its requirements
- complete any associated training
- seek clarification where required
- report concerns promptly.

Use of the school's digital systems confirms acceptance of the expectations contained within this policy.

Our Digital Commitment

At Bentham Community Primary School we believe that technology should strengthen education, improve communication and enhance opportunities for every child.

Every member of our workforce has a responsibility to use digital technology in ways that are:

- safe
- professional
- ethical
- secure
- inclusive
- responsible.

By working together, we will continue to create a digital culture that protects our children, supports our staff and reflects the values of our school community.

Appendix: Workforce Digital Code of Conduct

Our Ten Digital Commitments

Every member of staff at Bentham Community Primary School agrees to:

1. Put Children First

Use technology in ways that always protect, safeguard and promote the wellbeing of children.

2. Act Professionally

Remember that the same professional standards apply online as they do in person.

3. Protect Confidential Information

Keep personal and confidential information secure and only share it appropriately.

4. Use Artificial Intelligence Responsibly

Only use approved AI tools. Never upload confidential or personally identifiable information into public AI platforms. Always check AI-generated content for:

- accuracy
- bias
- safeguarding
- suitability.

5. Keep Systems Secure

- Use strong passwords
- Enable Multi-Factor Authentication
- Protect school devices
- Report suspicious activity immediately

6. Communicate Respectfully

Use professional language in emails, messaging, online meetings and digital platforms.

Think before sending.

7. Protect the School's Reputation

Remember that online behaviour can affect public confidence in the school. Avoid posting anything that could damage the reputation of colleagues, pupils or the school.

8. Report Concerns Immediately

Tell the Headteacher or appropriate leader if you become aware of:

- cyber attacks
- phishing
- data breaches
- safeguarding concerns
- misuse of AI
- lost devices.

9. Keep Learning

Technology changes quickly. Take part in training and remain up to date with cyber security, safeguarding and Artificial Intelligence.

10. Be Proud Digital Citizens

Help create a positive digital culture where technology supports learning, inclusion, creativity and collaboration. Every member of staff contributes to keeping our school community safe online.

Staff Declaration

I have read and understood the Workforce Digital Technology, Artificial Intelligence (AI) and Acceptable Use Policy.

I understand that:

- digital professionalism is part of my professional responsibilities;
- I remain accountable for all work produced using Artificial Intelligence;
- I will protect confidential information;
- I will follow the school's cyber security and safeguarding procedures;
- I will seek advice if I am unsure about the appropriate use of technology or AI.

Name: _____

Signature: _____

Date: _____