



BELMONT PRIMARY SCHOOL
Computing and Acceptable Use Policy

Signed by Chair of Governors:

Date approved by governors:

Reviewed: August 2026

Next Review: August 2027

1. Introduction

Digital technology is an important part of teaching, learning, communication and the day-to-day operation of Belmont Primary School. Used effectively, technology can enhance learning, support creativity and collaboration, improve communication and help prepare pupils to participate safely and confidently in an increasingly digital world.

The use of technology also presents potential risks, particularly in relation to safeguarding, online safety, data protection, cyber security and inappropriate or unlawful use. Belmont Primary School is committed to ensuring that technology is used safely, responsibly and appropriately by all members of the school community.

This policy sets out the expectations for the acceptable use of the school's digital technology, systems, networks and online services. It should be read alongside the school's safeguarding, behaviour, data protection and staff conduct policies.

2. Aims

This policy aims to:

- ensure that digital technology is used safely, responsibly and effectively to support teaching and learning;
- establish clear expectations for pupils, staff, governors, volunteers, contractors and visitors when using the school's digital systems and resources;
- promote safe, respectful and responsible behaviour online;
- protect pupils and staff from online harm and support the school's safeguarding responsibilities;
- protect the confidentiality, integrity and security of the school's information, systems and data;
- support compliance with relevant legislation and statutory guidance relating to safeguarding, data protection and the use of technology;
- ensure appropriate arrangements are in place for filtering and monitoring online activity;
- develop pupils' understanding of digital responsibility, online safety and the appropriate use of emerging technologies, including artificial intelligence (AI);
- reduce the risk of disruption, data loss, cyber attack or other harm arising from the misuse or attempted misuse of the school's systems; and
- provide a clear framework for responding to concerns or breaches of acceptable use.

3. Scope

This policy applies to all users of Belmont Primary School's digital technology and systems, including:

- pupils;
- teaching and support staff;
- governors;
- volunteers;
- contractors;
- visitors; and
- any other person authorised to access the school's systems or network.

For the purposes of this policy, digital technology includes school-owned or managed computers, laptops, tablets, mobile devices, telephones, networks, internet access, email, cloud-based services, software, applications, websites and other digital systems or services used by the school.

The policy applies to the use of school technology both on and off the school premises. It also applies, where relevant, to the use of personal devices or accounts where their use relates to school business, affects members of the school community, or has implications for safeguarding, professional conduct or the reputation of the school.

All users are expected to use technology in accordance with this policy and any relevant Acceptable Use Agreement.

Breaches of this policy will be considered in accordance with the circumstances and may be addressed through the school's Behaviour Policy, Staff Code of Conduct, disciplinary procedures, safeguarding procedures, Data Protection Policy or other relevant school procedures.

4. Roles and Responsibilities

Safe and effective use of digital technology is a shared responsibility. All members of the school community are expected to understand and follow the requirements of this policy appropriate to their role.

4.1 Governing Body

The Governing Body has overall responsibility for ensuring that appropriate arrangements are in place for the safe, secure and effective use of digital technology.

The Governing Body will:

- ensure that the school has appropriate policies and procedures relating to digital technology, online safety, data protection and cyber security;
- ensure that appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed regularly;
- ensure that the school meets relevant Department for Education filtering and monitoring standards;

- ensure that staff understand their responsibilities in relation to filtering and monitoring and receive appropriate training;
- provide appropriate challenge and oversight in relation to online safety, data security and cyber security; and
- review and approve this policy in accordance with the school's policy review cycle.

4.2 Headteacher

The Headteacher has overall operational responsibility for the implementation of this policy.

The Headteacher will:

- promote a culture in which digital technology is used safely, responsibly and effectively;
- ensure that staff understand and follow this policy and associated procedures;
- ensure that staff receive appropriate training and guidance;
- ensure that concerns or breaches relating to the use of digital technology are addressed appropriately;
- work with the Designated Safeguarding Lead (DSL), Computing Subject Lead, School Business Manager and ICT provider as appropriate; and
- ensure that appropriate resources are available to support the school's digital, safeguarding and cyber-security arrangements.

4.3 Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for safeguarding and online safety, including understanding the filtering and monitoring systems and processes in place within the school.

The DSL will:

- understand the school's filtering and monitoring arrangements and their role in protecting pupils from online harm;
- work with relevant staff and the school's ICT provider to identify and respond to safeguarding concerns arising from online activity;
- ensure that concerns identified through filtering or monitoring are acted upon appropriately;
- ensure that online-safety concerns are managed in accordance with the school's safeguarding and child protection procedures;
- support staff to recognise and report online-safety concerns; and
- contribute to the regular review of the effectiveness of the school's filtering and monitoring arrangements.

4.4 Computing Subject Lead

The Computing Subject Lead will support the effective and appropriate use of technology across teaching and learning.

The Computing Subject Lead will:

- oversee the implementation and development of the Computing curriculum;
- support staff in teaching pupils how to use technology safely, responsibly and effectively;
- promote progression in pupils' digital literacy and understanding of online safety;
- support the appropriate educational use of emerging technologies, including artificial intelligence;
- identify relevant training and development needs; and
- work with the Headteacher, DSL and ICT provider where curriculum use of technology has implications for safeguarding, security or acceptable use.

4.5 School Business Manager

The School Business Manager (SBM) will support the Headteacher in ensuring that the school's use of digital technology complies with its responsibilities relating to data protection, procurement, information security and business continuity.

The SBM will liaise with the school's ICT provider and other relevant services where necessary and will support the management of data breaches, cyber incidents and other information-security concerns in accordance with the school's relevant procedures.

4.6 ICT Provider

Belmont Primary School works with **OneIT** to support and maintain its ICT infrastructure and systems.

Working within the services agreed with the school, OneIT will support the school to:

- maintain the security and effective operation of its networks, systems and devices;
- manage appropriate user access and permissions;
- maintain appropriate technical filtering, monitoring and security measures;
- support software, security and system updates;
- support appropriate arrangements for backup and recovery;
- advise the school on identified technical or cyber-security risks;
- support the school in responding to significant ICT or cyber-security incidents; and

- provide technical advice to the Headteacher, DSL and other authorised staff as required.

4.7 Staff

All staff are responsible for using digital technology safely, professionally and in accordance with this policy.

Staff must:

- follow this policy, the Staff Code of Conduct and relevant data-protection and safeguarding procedures;
- use school systems, accounts and devices responsibly and securely;
- maintain the confidentiality and security of information to which they have access;
- follow the school's requirements relating to passwords, authentication and access controls;
- supervise and support pupils' appropriate use of technology;
- report safeguarding, online-safety, data-security or cyber-security concerns promptly through the appropriate school procedures;
- complete required training relating to online safety, data protection and cyber security; and
- model safe, respectful and responsible use of technology.

4.8 Pupils

Pupils are expected to:

- use school technology and internet access safely and responsibly;
- follow instructions given by staff about the use of devices, software, websites and online services;
- behave respectfully towards others when using technology;
- keep passwords and account details secure;
- tell a trusted member of staff if they encounter anything online that worries, upsets or concerns them;
- use artificial intelligence and other emerging technologies only in accordance with school expectations and staff guidance; and
- follow the Acceptable Use Agreement appropriate to their age.

The school will teach and support pupils to understand these responsibilities in an age-appropriate way.

4.9 Parents and Carers

Parents and carers have an important role in supporting safe and responsible use of technology.

The school asks parents and carers to:

- support the school's expectations for safe and responsible online behaviour;
- reinforce appropriate use of technology at home;
- raise concerns about online safety or the use of school technology with the school;
- communicate respectfully when using digital channels connected with the school; and
- support their child in understanding and following the school's Acceptable Use Agreement.

5. Acceptable Use of Digital Technology

Belmont Primary School provides access to digital technology, systems and internet services to support teaching, learning, communication and the effective operation of the school.

All users are expected to use these resources responsibly, safely, legally and in a manner consistent with the values and expectations of the school.

5.1 General Expectations

Users must:

- use school devices, systems, accounts and internet access primarily for educational or authorised school purposes;
- follow instructions and procedures relating to the safe and secure use of technology;
- use only accounts, systems, software and services that they are authorised to access;
- keep passwords and other login information secure and never use another person's account;
- respect the privacy, personal information and intellectual property of others;
- communicate respectfully and appropriately when using digital systems;
- take reasonable care of school equipment;
- report suspected security incidents, inappropriate content, accidental access to unsuitable material or other concerns promptly; and
- comply with any Acceptable Use Agreement applicable to their role.

Limited personal use of school systems by staff may be permitted where this is reasonable, does not interfere with their duties, does not incur additional cost to the school and complies with this policy and the Staff Code of Conduct.

5.2 Unacceptable Use

School technology, systems, networks and internet access must not be used to:

- access, create, download, store, share or distribute material that is illegal, discriminatory, defamatory, threatening, abusive, sexually explicit or otherwise inappropriate;
- bully, harass, intimidate or deliberately cause distress to another person;
- access or attempt to access accounts, files, data, systems or areas of the network without authorisation;
- disclose, share or misuse another person's personal or confidential information;
- impersonate another person or deliberately misrepresent the identity of the sender of a communication;
- bypass, disable or interfere with filtering, monitoring, security or access-control systems;
- introduce or deliberately spread malware, viruses or other harmful software;
- deliberately damage, disrupt or compromise school devices, networks, systems or data;
- install, download or use unauthorised software, applications, browser extensions or other digital services;
- infringe copyright, licensing or other intellectual-property rights;
- use school systems for unauthorised commercial activity, personal financial gain, gambling or party-political campaigning;
- engage in activity that could reasonably bring the school into disrepute; or
- undertake any activity that is unlawful or contrary to the school's safeguarding, behaviour or professional-conduct expectations.

Users must not attempt to circumvent restrictions simply because technical means of doing so are available.

5.3 Accidental Access to Inappropriate Material

The school recognises that inappropriate or unsuitable online content may occasionally be accessed unintentionally.

Where this occurs, users should:

- stop viewing the content;

- avoid sharing, copying or forwarding it; and
- report the incident promptly to an appropriate member of staff.

Pupils will be encouraged to report accidental access without fear of sanction where they have acted appropriately and honestly.

Any safeguarding concern arising from online content will be dealt with in accordance with the school's safeguarding and child protection procedures.

5.4 Monitoring of School Systems

Users should understand that use of school-owned or managed devices, accounts, networks and systems may be monitored where appropriate for safeguarding, security, technical, legal or operational purposes.

The school will undertake any monitoring proportionately and in accordance with its legal obligations, including those relating to data protection and privacy.

Users should therefore have no expectation that activity undertaken using school systems is entirely private.

6. Staff Use of Digital Technology

Staff are expected to use digital technology in a professional, responsible and secure manner. Use of technology must be consistent with this policy, the Staff Code of Conduct and the school's safeguarding and data-protection requirements.

6.1 Accounts, Passwords and Access

Staff must:

- use their own authorised account when accessing school systems;
- keep passwords and authentication information secure and not share them with others;
- use strong, unique passwords and follow any additional authentication requirements implemented by the school;
- lock or log out of devices when leaving them unattended;
- access only information, systems and files required for their role; and
- report any suspected unauthorised access, compromised account or security breach promptly.

Staff must not use another person's account or permit another person to use their account.

6.2 Email and Digital Communication

Staff must use their school email account or another school-approved communication system for communications relating to school business.

When communicating electronically, staff must:

- maintain the same professional standards expected in other forms of communication;
- take particular care when sending personal, sensitive or confidential information;
- check recipients carefully before sending messages or attachments;
- be alert to suspicious messages, links and attachments and report suspected phishing or other malicious communications;
- communicate with pupils and parents/carers only through school-approved channels; and
- maintain appropriate professional boundaries at all times.

Staff must not use personal social-media accounts, personal email accounts or other unauthorised messaging services to communicate privately with pupils.

6.3 Personal Devices

Personal mobile phones and other personal devices must be used in accordance with the Staff Code of Conduct and any other relevant school procedures.

Staff must not use personal devices to photograph, film or record pupils.

School information, particularly personal or confidential information, must not normally be stored on personal devices.

Where staff are permitted to access school systems using a personal device, they must follow the school's security requirements and take reasonable steps to prevent unauthorised access to school information.

6.4 Photographs, Video and Audio

Images, video or audio recordings of pupils must only be created, stored, used or shared for authorised school purposes and in accordance with the school's safeguarding, data-protection and consent arrangements.

School-approved devices and systems should be used for this purpose.

Staff must not publish or share images, recordings or information relating to pupils through personal accounts or unauthorised services.

6.5 Storage and Transfer of Information

Staff must use school-approved systems and services to store, access and transfer school information.

Personal or confidential information must not be transferred using unauthorised devices, accounts, applications or cloud-storage services.

Removable storage devices, such as USB drives, should only be used where necessary and must comply with the school's security requirements.

Staff must take particular care to ensure that information is not visible or accessible to unauthorised people when working away from school.

6.6 Remote Working and Remote Access

Remote access to school systems must only take place through methods authorised by the school and its ICT provider (OneIT).

When working remotely, staff must:

- take reasonable steps to ensure that school information cannot be seen or accessed by unauthorised people;
- use secure internet connections and school-approved systems;
- store school information securely;
- ensure devices are appropriately protected and kept up to date; and
- report the loss or theft of a device, or any suspected compromise of school information, immediately.

Staff must not deliberately bypass security controls or use unauthorised methods to access the school's network or systems remotely.

6.7 Software, Applications and Online Services

Staff must use software, applications and online services that have been approved for school use.

Staff should not create accounts for pupils, upload pupil information or introduce a new online service for school use without following the school's approval arrangements.

Particular care must be taken before entering personal, confidential or school information into online services, including artificial-intelligence tools.

Where staff are unsure whether a service is appropriate for use, they should seek advice before using it.

6.8 Reporting Concerns

Staff must report promptly:

- suspected data breaches or loss of personal information;
- lost or stolen school devices;
- suspected malware, phishing or compromised accounts;
- inappropriate or concerning online content;
- attempts to bypass the school's filtering or security arrangements; and
- any use of technology that gives rise to a safeguarding concern.

Safeguarding concerns must be reported in accordance with the school's safeguarding and child protection procedures. Technical and security concerns should be reported through the school's established arrangements with OneIT and, where appropriate, to the Headteacher or School Business Manager.

7. Pupil Use of Digital Technology

Belmont Primary School recognises that digital technology provides valuable opportunities for pupils to learn, communicate, create and develop the knowledge and skills they need to participate safely and confidently in the digital world.

Pupils will be taught to use technology safely, respectfully, responsibly and appropriately. Expectations will reflect pupils' age and understanding and will be reinforced through the Computing curriculum, online-safety education and wider school life.

7.1 Access to Technology

Pupils may use school devices, systems, internet access, software and online services for educational purposes and as directed by staff.

Pupils must:

- follow staff instructions when using technology;
- use only the devices, accounts, applications and services they have been authorised to use;
- use their own account and keep passwords secure;
- take reasonable care of school equipment;
- respect the work, files and information of others;
- use technology in a kind, respectful and responsible way; and
- follow the Acceptable Use Agreement appropriate to their age.

Access to particular websites, applications, services or features may be restricted according to pupils' age, educational need and the school's safeguarding and security arrangements.

7.2 Online Behaviour

The same standards of behaviour expected in school apply when pupils use technology.

Pupils must not use digital technology to:

- bully, threaten, harass or deliberately upset another person;
- send or share unkind, offensive or inappropriate messages or material;
- impersonate another person or use another person's account;
- deliberately access, create or share inappropriate or harmful content;

- disclose their own or another person's personal information without permission;
- take, use or share photographs, video or audio recordings without appropriate permission;
- deliberately damage or interfere with devices, files, systems or networks; or
- attempt to bypass the school's filtering, monitoring or security arrangements.

Concerns about pupils' online behaviour will be addressed in accordance with the school's Behaviour Policy and, where appropriate, its safeguarding and child protection procedures.

7.3 Online Safety Education

The school will provide age-appropriate opportunities for pupils to learn about online safety and digital responsibility.

This will include teaching pupils to:

- recognise that information found online may be inaccurate, misleading or deliberately false;
- consider whether online information and sources are reliable;
- understand that people online may not always be who they claim to be;
- protect personal information and understand the importance of privacy;
- recognise inappropriate, harmful or upsetting content and behaviour;
- understand the potential consequences of sharing information, images or messages online;
- behave respectfully towards others online;
- understand that online activity can leave a digital record;
- recognise when something online makes them feel worried, uncomfortable or unsafe; and
- know how and when to seek help from a trusted adult.

7.4 Reporting Online Concerns

Pupils are encouraged to tell a trusted adult immediately if they:

- see or receive something online that worries, frightens or upsets them;
- are contacted in a way that makes them uncomfortable;
- experience or witness online bullying or other inappropriate behaviour;
- accidentally access inappropriate content;
- believe somebody else may be at risk; or

- make a mistake while using technology and need help.

Pupils will be supported to understand that **reporting a concern or an honest mistake is the right thing to do.**

Staff will respond to concerns in an age-appropriate and proportionate way and will follow safeguarding procedures where necessary.

7.5 Personal Devices

Pupils may only bring or use personal devices in school in accordance with the school's agreed rules and with permission where required.

Where a personal device is permitted, its use remains subject to the school's expectations for behaviour, safeguarding and acceptable use while on school premises or being used in connection with school activities.

The school may restrict or withdraw permission to use a personal device where its use is inappropriate, unsafe or disruptive.

7.6 Acceptable Use Agreements

Pupils will be introduced to an age-appropriate Acceptable Use Agreement which explains the school's expectations in language they can understand.

The agreements will be used as part of the school's education about safe and responsible use of technology rather than simply as a list of prohibited activities.

Parents and carers will be encouraged to discuss these expectations with their child and support their safe and responsible use of technology.

8. Artificial Intelligence (AI)

Belmont Primary School recognises that artificial intelligence (AI) is an increasingly important part of the digital world and has the potential to support teaching, learning, creativity and school administration when used appropriately.

The school will take a balanced approach to AI. Pupils and staff should be supported to understand both its potential benefits and its limitations and risks. AI will not be treated as inherently unsafe or inappropriate; however, its use must be purposeful, age-appropriate, secure and consistent with the school's safeguarding, data-protection and professional expectations.

8.1 Principles for the Use of AI

When using AI tools for school purposes, users should:

- have a clear and appropriate educational or professional purpose for their use;
- use only AI tools or services that are appropriate for the task and, where required, approved by the school;
- protect personal, confidential and sensitive information;

- critically evaluate AI-generated information rather than assuming that it is accurate;
- recognise that AI-generated content may contain errors, bias, inappropriate material or fabricated information;
- respect copyright and intellectual-property rights;
- be open and transparent about significant use of AI where this is relevant to the work being produced; and
- remain responsible for decisions, work and content produced with the assistance of AI.

AI should support human judgement, creativity and learning rather than replace them.

8.2 Staff Use of AI

Staff may use appropriate AI tools where there is a clear educational or professional benefit and their use is consistent with school requirements.

Staff must not enter personal, confidential or sensitive information about pupils, families, staff or the school into an AI tool unless the tool has been specifically approved for that purpose and appropriate data-protection arrangements are in place.

Staff using AI-generated material must:

- check it carefully for accuracy, appropriateness and bias before use;
- ensure that materials are suitable for the age, needs and circumstances of pupils;
- exercise their own professional judgement rather than relying solely on an AI-generated recommendation or decision;
- ensure that AI is not used to make significant decisions about an individual pupil or member of staff without appropriate human oversight; and
- consider copyright, intellectual property and data-protection requirements when creating or using AI-generated content.

AI-generated lesson plans, resources, correspondence, assessments or other materials remain the responsibility of the member of staff who chooses to use them.

8.3 Pupil Use of AI

Pupils may use AI tools for educational purposes where this has been permitted or directed by a member of staff and the tool is appropriate for their age.

The school will teach pupils that AI can be useful for activities such as exploring ideas, asking questions, developing understanding and supporting creativity, but that its answers should not automatically be trusted.

Pupils will be taught to:

- question and check information produced by AI;

- compare information with other reliable sources where appropriate;
- recognise that AI can make mistakes or produce convincing information that is untrue;
- use AI to support their thinking rather than avoid learning or doing the work themselves;
- follow staff instructions about when AI may or may not be used;
- be honest about their use of AI when completing schoolwork; and
- never enter their own or another person's private or personal information into an AI tool.

Pupils must not use AI to impersonate, bully, deceive or deliberately cause harm to another person, or to create or distribute inappropriate content.

8.4 AI and Pupils' Work

The appropriate use of AI will depend on the purpose of the activity and the guidance given by the member of staff.

Where independent work is required, pupils must not use AI to generate work and present it as entirely their own.

Where AI use is permitted, pupils may be asked to explain how they used it, what it contributed and how they checked or developed the resulting work.

The school's response to inappropriate use of AI will take account of the pupil's age, understanding, the guidance they were given and whether the misuse was deliberate.

8.5 Mistakes and Concerns

Pupils and staff are encouraged to report concerns arising from the use of AI, including unexpected or inappropriate content, inaccurate or concerning responses, accidental disclosure of information or uncertainty about whether a tool is appropriate.

A pupil who encounters inappropriate AI-generated content or makes an honest mistake and reports it should be supported in the same way as a pupil who reports other online-safety concerns.

Deliberate misuse will be addressed appropriately, but the school will seek to maintain a culture in which pupils feel safe to ask for help and report concerns.

8.6 Keeping the School's Approach Under Review

AI technology is developing rapidly. The school will keep its use of AI and the associated opportunities and risks under review and will update guidance, training and approved practice as necessary.

The school may restrict or withdraw access to particular AI tools where there are concerns relating to age appropriateness, safeguarding, privacy, data protection, security or educational suitability.

9. Online Safety, Filtering and Monitoring

Belmont Primary School is committed to providing pupils and staff with safe and appropriate access to online resources while recognising that no technical system can remove all online risk.

The school uses filtering and monitoring systems as part of its wider safeguarding arrangements. These systems are intended to reduce the risk of access to harmful or inappropriate content and to help identify online activity that may indicate a safeguarding, welfare or security concern.

Technical filtering and monitoring arrangements are managed and supported through the school's ICT provider, OneIT. Responsibility for safeguarding pupils and responding appropriately to concerns remains with Belmont Primary School.

9.1 Filtering

The school's internet connection and network are subject to appropriate filtering controls.

Filtering arrangements will seek to:

- block access to illegal, harmful and inappropriate online content;
- protect pupils from content that may present a safeguarding risk;
- reflect the age and needs of pupils at Belmont Primary School;
- allow appropriate access to educational material without unreasonably restricting teaching and learning; and
- prevent users from deliberately bypassing or disabling filtering controls.

Filtering will be applied appropriately to school-managed devices and internet access.

The school recognises that filtering cannot identify or prevent every potential risk. It will therefore be used alongside effective supervision, online-safety education, appropriate staff practice and the school's wider safeguarding arrangements.

9.2 Monitoring

The school uses appropriate technical monitoring to help identify activity on its systems that may give rise to safeguarding, welfare, behavioural or security concerns.

Monitoring may identify potentially concerning search terms or online activity undertaken by pupils or staff and generate alerts for review.

Alerts do not, in themselves, establish that inappropriate behaviour or a safeguarding incident has occurred. Any alert or concern will be considered in context and responded to proportionately.

Where an alert indicates a potential safeguarding concern, it will be referred promptly to the Designated Safeguarding Lead (DSL) or a Deputy DSL and dealt with in accordance with the school's safeguarding and child protection procedures.

Technical or cyber-security concerns will be referred to OneIT and appropriate school staff as necessary.

9.3 Responsibilities

The Governing Body will ensure that appropriate filtering and monitoring arrangements are in place and that their effectiveness is reviewed.

The Headteacher will ensure that filtering and monitoring arrangements are implemented effectively and that relevant staff understand their responsibilities.

The DSL will take lead responsibility for understanding the safeguarding implications of filtering and monitoring and for ensuring that safeguarding concerns identified through these systems are responded to appropriately.

OneIT will provide technical support for the school's filtering and monitoring systems in accordance with the school's agreed service arrangements, including the management of technical controls and the generation or routing of relevant alerts.

All staff must:

- understand the purpose of the school's filtering and monitoring arrangements;
- remain vigilant when pupils are using technology and not rely solely on technical controls;
- act promptly where they observe or become aware of concerning online activity;
- report safeguarding concerns in accordance with school procedures; and
- report apparent weaknesses, failures or inappropriate blocking within the filtering and monitoring systems.

9.4 Responding to Alerts and Concerns

Where potentially concerning online activity is identified, the school will consider the nature and context of the activity before determining the appropriate response.

This may include:

- speaking with the pupil or member of staff concerned;
- reviewing relevant information to establish the context;
- making a safeguarding referral within school;
- providing support or additional online-safety education;
- addressing deliberate misuse through the appropriate behaviour or staff procedure;

- seeking technical advice or action from OneIT; or
- making an external referral where this is required to safeguard a child or another person.

The school's response will distinguish, as far as reasonably possible, between deliberate misuse, genuine curiosity, accidental access and activity that may indicate that an individual needs help or support.

A pupil will not be discouraged from reporting a concern because they are worried that the search, content or activity which led to it may itself result in punishment.

9.5 Review of Filtering and Monitoring

The school will review the effectiveness of its filtering and monitoring arrangements regularly and at least annually.

The review will consider whether:

- the systems remain appropriate for the age and needs of pupils;
- harmful and inappropriate content is being blocked effectively;
- appropriate educational content remains accessible;
- monitoring and alert arrangements are operating effectively;
- safeguarding concerns are being identified and responded to appropriately;
- staff understand their roles and responsibilities; and
- any changes to technology, patterns of use or emerging risks require the school's arrangements to be adjusted.

The school will work with OneIT to address technical issues or improvements identified through this review.

Significant concerns, incidents or changes to the school's systems may result in an additional review being undertaken before the next scheduled review.

10. Data Security and Cyber-Security

Belmont Primary School recognises that effective data and cyber security is essential to protecting pupils, staff, school information and the continuity of the school's operations.

The school will take appropriate organisational and technical measures to protect its systems and information from accidental loss, unauthorised access, misuse, damage and cyber attack.

Technical security arrangements are supported and managed through the school's ICT provider, OneIT. All users also have an important role in maintaining security through safe and responsible practice.

10.1 Access and Authentication

Access to school systems and information will be limited according to the needs and responsibilities of each user's role.

Users must:

- access systems only through their own authorised accounts;
- use strong, unique passwords and comply with the school's password requirements;
- keep passwords and authentication information confidential;
- use multi-factor authentication (MFA) where this is provided or required;
- lock or log out of devices when they are left unattended; and
- report suspected unauthorised access or compromised account details immediately.

Access rights will be reviewed and amended where roles change and removed promptly when access is no longer required.

10.2 Devices and Software

School-managed devices will be appropriately configured and protected.

The school, working with OneIT, will ensure that appropriate arrangements are in place for:

- security updates and software patches;
- malware and virus protection;
- device and network security;
- appropriate access controls;
- supported and appropriately licensed software; and
- the removal or secure management of devices and software that are no longer supported.

Users must not deliberately disable, remove or circumvent security controls or install unauthorised software.

10.3 Protecting School Information

Personal, confidential and sensitive information must be handled in accordance with the school's Data Protection Policy and associated procedures.

Users must:

- access personal information only where this is necessary for their role;
- use school-approved systems to store and share school information;

- take appropriate care when sending information electronically;
- check recipients before sending personal or confidential information;
- avoid leaving confidential information visible or accessible to unauthorised people;
and
- securely dispose of information when it is no longer required, in accordance with the school's retention arrangements.

Personal or confidential school information must not be uploaded to unauthorised websites, applications, cloud-storage services or AI tools.

10.4 Removable Media

The use of removable storage devices, including USB drives, will be minimised where secure school-approved alternatives are available.

Where removable media is required, it must be used in accordance with the school's security arrangements.

Personal or confidential information must not be stored on an unencrypted removable device.

Unknown or untrusted removable devices must not be connected to school equipment.

10.5 Backups, Recovery and Business Continuity

The school will maintain appropriate arrangements for the backup and recovery of important systems and information as part of its wider business continuity arrangements.

Belmont Primary School's technical backup and disaster-recovery arrangements are provided and supported through OneIT. Detailed technical arrangements are maintained separately within the school's Business Continuity and Disaster Recovery documentation and will be reviewed with OneIT as appropriate.

The school, working with OneIT and other relevant service providers, will ensure that:

- important data is backed up appropriately;
- backups are appropriately protected from unauthorised access and cyber attack;
- appropriate recovery arrangements are in place;
- data loss, system failure or other incidents requiring recovery are reported promptly;
and
- backup and recovery arrangements are reviewed or tested as appropriate.

10.6 Phishing and Malicious Communications

All users should be alert to phishing, fraudulent messages and other attempts to obtain information or compromise school systems.

Staff must:

- treat unexpected requests for passwords, payments or sensitive information with caution;
- check unusual or unexpected requests through an independent means where appropriate;
- avoid opening suspicious links or attachments; and
- report suspected phishing or malicious communications promptly.

Where a user believes they may have clicked a malicious link, opened a harmful attachment or disclosed account information, they should report this **immediately rather than attempting to conceal or resolve the issue themselves**.

Prompt reporting enables the school and OneIT to take action to reduce potential harm.

10.7 Security Incidents and Data Breaches

Suspected cyber-security incidents, loss of information, unauthorised disclosure, compromised accounts and lost or stolen devices must be reported promptly.

The school will assess the nature and potential impact of an incident and will involve the Headteacher, School Business Manager, DSL, OneIT, Data Protection Officer or other relevant personnel as appropriate.

Where required, incidents will be managed in accordance with the school's data-breach, safeguarding and business-continuity arrangements and reported to external bodies where there is a legal or regulatory requirement to do so.

Users should preserve relevant information and follow instructions given during the management of an incident.

10.8 Cyber-Security Awareness

Staff will receive appropriate information and training to help them recognise and respond to cyber-security risks.

This will include, as appropriate:

- password and account security;
- multi-factor authentication;
- phishing and fraudulent communications;
- safe handling of personal and confidential information;

- use of devices and remote access;
- reporting security incidents; and
- emerging cyber-security risks.

The school will promote a culture in which users report mistakes and suspected incidents promptly so that action can be taken quickly.

Deliberate or reckless breaches of security requirements may be addressed under the appropriate school procedure.

11. Email, Digital Communication and Social Media

Digital communication can support effective communication between the school, staff, pupils, parents/carers and the wider community. All users must communicate appropriately, professionally and with due regard to safeguarding, confidentiality and privacy.

11.1 School Email and Communication Systems

Staff must use school-approved communication systems for school business and when communicating with pupils and parents/carers in a professional capacity.

Staff must:

- communicate in a professional, respectful and appropriate manner;
- use their school email account or another school-approved system for school-related communication;
- take care when sending personal, sensitive or confidential information;
- check recipients before sending emails, messages or attachments;
- use appropriate security measures when sharing confidential information;
- be alert to phishing, suspicious links, attachments and fraudulent requests; and
- report messages or communications that give rise to safeguarding, data-protection or cyber-security concerns.

School email accounts and communication systems must not be used to send or distribute offensive, discriminatory, defamatory, threatening or otherwise inappropriate material.

11.2 Communication with Pupils

Staff must maintain appropriate professional boundaries when communicating electronically with pupils.

Communication with pupils must:

- have a clear and legitimate educational or pastoral purpose;
- take place through school-approved systems;

- be appropriate in tone, content and timing; and
- comply with the Staff Code of Conduct and safeguarding procedures.

Staff must not communicate privately with pupils through personal social-media accounts, personal email addresses, personal messaging accounts or other unauthorised channels.

Where pupils contact a member of staff through an inappropriate personal channel, the member of staff should not continue the communication and should report the contact where there is a safeguarding or professional-boundary concern.

11.3 Communication with Parents and Carers

Staff should communicate with parents and carers through the school's approved communication channels.

Communication should remain professional and should not disclose information about other pupils, families or members of staff.

Staff should be mindful that written digital communications may be retained, forwarded or shared and should therefore apply the same professional standards to electronic communication as they would to a formal letter or face-to-face conversation.

11.4 Social Media

Staff use of social media must also comply with the professional standards and expectations set out in the Staff Code of Conduct, including those relating to confidentiality, professional boundaries, contact with pupils and parents/carers, the use of images and conduct which may affect the reputation of the school.

Staff must:

- maintain appropriate professional boundaries online;
- take reasonable steps to manage the privacy and security of personal social-media accounts;
- avoid sharing confidential or sensitive information obtained through their work;
- not publish photographs, recordings or personal information about pupils through personal accounts;
- not use social media to discuss individual pupils, parents/carers, colleagues or confidential school matters;
- not engage in online behaviour that could reasonably call into question their suitability to work with children or their professional conduct; and

Staff should be aware that privacy settings cannot guarantee that material posted online will remain private.

11.5 Online Connections with Pupils and Parents/Carers

Staff must not accept or initiate personal social-media connections with current pupils.

Staff should exercise professional judgement and appropriate caution in relation to personal social-media connections with parents and carers, recognising the potential for blurred professional boundaries, conflicts of interest or unintended disclosure of personal information.

Where social media is used by the school for official communication or publicity, it must be through an authorised school account managed in accordance with school procedures.

11.6 School Social-Media Accounts

Only authorised members of staff may create, administer or publish content through an official Belmont Primary School social-media account.

Content published on behalf of the school must:

- be appropriate and consistent with the school's values;
- protect pupils' and staff members' privacy;
- comply with relevant consent and data-protection arrangements;
- avoid disclosing confidential information; and
- be suitable for publication to a potentially unrestricted audience.

Access details for official accounts must be managed securely and must not be shared with unauthorised users.

11.7 Concerns and Inappropriate Online Communication

Staff who become aware of online content or communication that may constitute a safeguarding concern, breach confidentiality, threaten the security of school systems or seriously affect a member of the school community should report it through the appropriate school procedure.

The school will respond according to the nature and seriousness of the concern and may use its safeguarding, behaviour, disciplinary, complaints or other relevant procedures as appropriate.

12. Personal Devices and Remote Access

The use of personal devices and remote access to school systems must not compromise safeguarding, professional boundaries, data protection or the security of the school's information and systems.

Staff use of personal devices must also comply with the relevant expectations set out in the Staff Code of Conduct.

12.1 Staff Personal Devices

Personal mobile phones, tablets, laptops, smartwatches and other personal devices must be used responsibly and in accordance with school expectations.

Staff must:

- follow the Staff Code of Conduct regarding when and where personal devices may be used during the working day;
- ensure that personal-device use does not interfere with their professional responsibilities or the supervision of pupils;
- keep personal devices secure where they are brought onto school premises;
- not use personal devices to photograph, film or record pupils;
- not store personal or confidential school information on personal devices unless specifically authorised and appropriate security arrangements are in place; and
- not use personal accounts or applications for school communication where an approved school system is available.

Personal devices must not be connected to school systems or used in a way that circumvents the school's security, filtering or monitoring arrangements.

12.2 Pupil Personal Devices

Pupils may only bring personal devices onto school premises in accordance with the school's agreed arrangements.

Where permission has been given for a pupil to bring a device into school, the pupil must follow staff instructions regarding its storage and use.

Personal devices must not be used by pupils to photograph, film or record other members of the school community without permission.

The school may restrict or withdraw permission to bring or use a personal device where its use presents a safeguarding concern, disrupts learning or breaches school expectations.

12.3 Visitors, Volunteers and Contractors

Visitors, volunteers and contractors must use personal devices in a way that does not compromise safeguarding, confidentiality or the security of the school.

They must not photograph, film or record pupils unless specifically authorised to do so for an agreed purpose.

Access to the school's network or systems will only be provided where necessary and appropriate.

12.4 Remote Access

Remote access to school systems will only be provided where there is an appropriate operational need and through methods authorised by Belmont Primary School and OneIT.

Users accessing school systems remotely must:

- use only authorised accounts and access methods;
- comply with password and multi-factor authentication requirements;
- take reasonable steps to prevent school information being seen or accessed by unauthorised people;
- use secure devices and internet connections;
- not download or store personal or confidential information unnecessarily;
- lock or log out of systems when they are not in use; and
- report lost devices, compromised accounts or other security concerns immediately.

Remote access privileges may be restricted or withdrawn where they are no longer required or where there is a safeguarding or security concern.

12.5 Working Away from School

Staff working away from the school site remain responsible for protecting school information and maintaining appropriate professional standards.

Particular care should be taken when working in public or shared spaces to ensure that conversations, screens and documents containing personal or confidential information cannot be seen or overheard by others.

School information should be accessed, stored and shared through approved systems wherever possible.

13. Responding to Concerns and Misuse

Belmont Primary School will respond to concerns about the use of digital technology in a fair, proportionate and appropriate manner.

The school's response will take account of the nature and seriousness of the concern, the individual's age and understanding, the circumstances in which it occurred and any potential safeguarding, welfare, data-protection or security implications.

The school recognises an important distinction between an honest mistake or accidental access, behaviour arising from curiosity or limited understanding, activity that may indicate a safeguarding or welfare concern, and deliberate, reckless or malicious misuse.

13.1 Accidental Access and Honest Mistakes

Users are expected to report accidental access to inappropriate content, mistaken disclosure of information, suspicious communications and other digital mistakes promptly.

Where a pupil or member of staff makes an honest mistake and reports it appropriately, the school's priority will normally be to:

- ensure that the individual and others are safe;
- limit or remedy any potential harm;
- provide appropriate advice, support or education;
- address any technical or security issue; and
- consider whether any wider action is necessary.

The school will seek to maintain a culture in which users feel able to report mistakes promptly rather than concealing them through fear of blame or sanction.

This does not prevent the school from addressing repeated carelessness or behaviour where reasonable instructions or security requirements have not been followed.

13.2 Safeguarding and Welfare Concerns

Online activity that initially appears to be inappropriate use may sometimes indicate that a pupil is experiencing, witnessing or at risk of harm.

Where digital activity, searches, messages, images, communications or other information raise a safeguarding concern, the matter will be referred to the DSL or a Deputy DSL and considered in accordance with the school's safeguarding and child protection procedures.

The need to understand and safeguard the child will take priority over treating the activity simply as a breach of acceptable use.

Where appropriate, pupils will be offered support and additional education to help them understand and manage online risks.

13.3 Pupil Misuse

Where a pupil deliberately misuses digital technology, the school will respond in accordance with its Behaviour Policy and other relevant procedures.

The response will take account of:

- the pupil's age and level of understanding;
- whether the behaviour was deliberate;
- the nature and seriousness of the misuse;
- whether another person has been harmed or placed at risk;
- whether the behaviour has occurred previously;
- any relevant additional needs or circumstances; and
- any safeguarding concerns arising from the incident.

Possible responses may include:

- discussion, guidance or additional online-safety education;
- restorative action where another person has been affected;
- increased supervision or temporary restrictions on access to particular technology;
- consequences in accordance with the Behaviour Policy;
- involvement of parents/carers;
- safeguarding action; or
- referral to an external agency where necessary.

Restrictions on access to technology should be proportionate and should not unnecessarily prevent a pupil from accessing learning.

13.4 Staff Misuse

Concerns about staff use of digital technology will be considered in accordance with the Staff Code of Conduct and, where appropriate, the school's safeguarding, disciplinary, data-protection or other relevant procedures.

The response will take account of the nature and seriousness of the concern and whether the conduct was accidental, negligent, reckless or deliberate.

Where an allegation or concern relates to the safeguarding of children, it will be managed in accordance with the school's safeguarding procedures.

Nothing in this policy replaces or overrides the professional expectations contained within the Staff Code of Conduct.

13.5 Security and Data Incidents

Where misuse has resulted in, or may result in, a cyber-security incident, data breach or compromise of school systems, the school will take prompt action to contain and assess the incident.

OneIT and other relevant personnel will be involved as appropriate.

The immediate priority will be to protect individuals, information and systems and to prevent further harm. Any consideration of disciplinary or behavioural consequences can take place once appropriate protective action has been taken.

13.6 Serious or Unlawful Misuse

Serious incidents may require referral to an external agency.

This may include circumstances involving:

- suspected criminal activity;
- significant safeguarding concerns;
- threats of serious harm;
- sexual abuse or exploitation;
- illegal or seriously harmful online content;
- serious harassment or malicious communications;
- significant unauthorised access to or interference with computer systems; or
- a serious breach of personal or confidential information.

The Headteacher and DSL will determine the appropriate course of action, seeking advice from relevant professionals or agencies where necessary.

The school will preserve relevant information or evidence where this may be required for a safeguarding investigation, disciplinary process or external investigation.

13.7 Restricting Access

The school reserves the right to restrict, suspend or withdraw access to its devices, systems, accounts or network where this is necessary to protect pupils, staff, information or the security and effective operation of the school.

Any restriction will be proportionate to the circumstances and kept under review.

Where access is required for a pupil's education or a member of staff's role, reasonable alternative arrangements will be considered where appropriate.

14. Monitoring and Review

The Headteacher has overall responsibility for monitoring the implementation and effectiveness of this policy.

The policy will be reviewed regularly and at least annually, with input from the Designated Safeguarding Lead (DSL), Computing Subject Lead, School Business Manager, OneIT and other relevant staff as appropriate.

The review will take account of:

- changes to legislation, statutory guidance and national standards;
- developments in technology and emerging digital risks;
- safeguarding and online-safety concerns;

- the effectiveness of filtering and monitoring arrangements;
- cyber-security incidents and identified vulnerabilities;
- developments in artificial intelligence and other emerging technologies;
- feedback from staff, pupils and other members of the school community where appropriate; and
- lessons arising from incidents or the implementation of this policy.

The policy may be reviewed earlier where there is a significant change to legislation, guidance, technology, school systems or identified risk.

Any significant changes to the policy will be approved in accordance with the school's usual governance arrangements.

15. Legal and Guidance Framework

This policy has been developed with regard to relevant legislation, statutory guidance and national standards, including:

- Keeping Children Safe in Education;
- the Department for Education's filtering and monitoring standards for schools and colleges;
- the Department for Education's digital and technology standards for schools and colleges;
- the Education Act 2011;
- the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR);
- the Computer Misuse Act 1990;
- the Copyright, Designs and Patents Act 1988;
- the Equality Act 2010; and
- relevant Department for Education guidance concerning the use of generative artificial intelligence in education.

The school will have regard to updated or replacement legislation, statutory guidance and national standards where these are introduced during the lifetime of this policy.

16. Related Policies and Procedures

This policy should be read alongside other relevant Belmont Primary School policies and procedures, including:

- Child Protection and Safeguarding Policy;
- Staff Code of Conduct;
- Behaviour Policy;
- Data Protection Policy;
- Records Management and Retention arrangements;
- Freedom of Information Policy;
- Remote Learning arrangements, where applicable;
- Business Continuity and Disaster Recovery arrangements; and
- any other school procedures relating to online safety, information security or the use of digital technology.

Where a concern involving digital technology also raises a safeguarding, conduct, behaviour, data-protection or security issue, the relevant school policy or procedure will apply alongside this policy.

Appendix 1 – Staff Acceptable Use Agreement

Digital technology is an important part of teaching, learning and the effective operation of Belmont Primary School. All staff have a responsibility to use technology safely, professionally and securely and to model appropriate digital behaviour for pupils.

This agreement should be read alongside the **Computing and Acceptable Use Policy**, **Staff Code of Conduct**, **Child Protection and Safeguarding Policy** and **Data Protection Policy**.

By signing this agreement, I confirm that I understand and agree to the following expectations.

I will:

- use school devices, systems, accounts and internet access responsibly and primarily for authorised school purposes;
- use my own authorised account and keep my passwords and authentication details secure;
- use strong, unique passwords and multi-factor authentication where required;
- lock or log out of devices when leaving them unattended;
- use school-approved systems for school-related communication and the storage and sharing of school information;
- maintain appropriate professional boundaries when communicating electronically with pupils and parents/carers;
- take appropriate care when handling personal, sensitive or confidential information;
- check recipients carefully before sending emails, messages or attachments containing personal or confidential information;
- take reasonable steps to protect school information when working remotely or away from the school site;
- follow the school's expectations relating to personal devices, photographs, video and audio recordings;
- use only software, applications, online services and AI tools that are appropriate for school use;
- critically check AI-generated information or materials before using them and remain professionally responsible for any content I choose to use;
- follow school requirements relating to safeguarding, online safety, filtering and monitoring;
- remain vigilant when pupils are using technology and not rely solely on technical filtering and monitoring systems;
- report safeguarding concerns promptly in accordance with the school's safeguarding procedures;
- report suspected phishing, malware, compromised accounts, lost devices, data loss, data breaches or other security concerns promptly;
- report accidental access to inappropriate material or other honest mistakes so that appropriate action can be taken;
- respect copyright, intellectual-property rights and software licensing requirements;
- and

- follow reasonable instructions from the school and OneIT relating to the safe and secure use of technology.

I will not:

- share my password or knowingly allow another person to use my account;
- access accounts, information, files or systems that I am not authorised to access;
- attempt to bypass or interfere with the school's filtering, monitoring or security controls;
- install or use unauthorised software, applications, browser extensions or online services;
- use personal email, personal social-media accounts or unauthorised messaging services to communicate privately with pupils;
- use a personal device to photograph, film or record pupils;
- publish or share information, photographs or recordings relating to pupils through personal accounts or unauthorised services;
- store personal or confidential school information on unauthorised devices or services;
- enter personal, confidential or sensitive information about pupils, families, staff or the school into an AI tool unless that tool has been specifically approved for that purpose;
- use school technology to access, create, store or distribute illegal, offensive, discriminatory, abusive or otherwise inappropriate material;
- deliberately introduce malware or undertake any action intended to compromise or disrupt school systems; or
- use technology in a way that breaches the Staff Code of Conduct or could compromise safeguarding, confidentiality, professional boundaries or the security of the school.

Reporting Concerns and Mistakes

I understand that I am expected to report concerns, suspected security incidents and honest mistakes promptly.

I understand that the school's priority following an accidental or suspected security incident will be to protect pupils, staff, information and systems and to limit any potential harm.

I understand that deliberately concealing an incident may increase the risk to the school and others.

Monitoring

I understand that activity undertaken using school-owned or managed devices, accounts, networks and systems may be filtered and monitored for safeguarding, security, technical, legal and operational purposes.

I understand that I should not expect activity undertaken using school systems to be entirely private.

Agreement

I understand that access to the school's digital technology and systems is provided to support my work at Belmont Primary School and that I am responsible for using these resources appropriately.

I understand that deliberate, reckless or serious misuse may result in access being restricted or withdrawn and may be addressed under the Staff Code of Conduct, safeguarding, disciplinary, data-protection or other relevant school procedures.

Name: _____

Role: _____

Signature: _____

Date: _____

Appendix 2 – EYFS and Key Stage 1 Acceptable Use Agreement

My Safe and Happy Technology Rules

We use computers, tablets and the internet to help us learn and have fun.

When I use technology at Belmont Primary School, I will try to follow these rules:

I will:

- **ask a grown-up** before I use a computer, tablet, website or app;
- use technology for the things my teacher asks me to do;
- be **kind and respectful** to other people when I am using technology;
- look after computers, tablets and other equipment;
- keep my password private and only use **my own** account;
- ask before I take or share a photograph, video or recording;
- keep personal information, such as my full name, address and passwords, private;
- remember that things I see or hear online **might not always be true**;
- tell a trusted grown-up if I see or hear something online that makes me feel **worried, frightened, confused or uncomfortable**; and
- tell a grown-up if I make a mistake or something goes wrong.

If something goes wrong...

I will tell a grown-up.

I know that I can ask for help if I click on something by mistake or see something I should not have seen.

Telling a grown-up is the right thing to do.

My teachers will help me learn how to use technology safely and responsibly.

My agreement

I have talked about these rules with an adult and I will try my best to follow them.

Pupil's name: _____

Pupil's signature/name or mark: _____

Date: _____

Parent/Carer

I have discussed these rules with my child and will support the school's approach to safe and responsible use of technology.

Parent/Carer's name: _____

Signature: _____

Date: _____

Appendix 3 – Key Stage 2 Acceptable Use Agreement

Using Technology Safely and Responsibly

At Belmont Primary School, we use computers, tablets, the internet and other digital technology to help us learn, communicate and be creative.

Technology can be extremely useful, but we all have a responsibility to use it safely, respectfully and responsibly.

By following this agreement, I am helping to keep **myself and other people safe**.

When I use technology at school, I will:

- use school devices, accounts, websites and apps for learning and for activities approved by my teacher;
- follow instructions given by staff about how and when technology should be used;
- use my own account and keep my password private;
- treat school devices and equipment carefully;
- be kind and respectful when communicating with or about other people online;
- respect other people's files and personal information;
- think carefully before sharing information, messages, photographs or other content;
- ask permission before taking, using or sharing a photograph, video or recording of another person;
- keep personal information private and think carefully about what is safe to share online;
- remember that people online may not always be who they say they are;
- remember that information I find online may not always be accurate or true;
- check information using reliable sources when appropriate;
- respect other people's work and understand that I should not copy work and pretend it is my own;
- tell a trusted adult if I see, receive or find something online that worries, frightens, upsets or confuses me; and
- tell a member of staff if I make a mistake or something goes wrong.

I will not:

- use another person's account or try to find out their password;
- deliberately access another person's files or information without permission;
- use technology to bully, threaten, embarrass or deliberately upset another person;
- create, search for, access or share inappropriate or harmful content deliberately;
- share my own or another person's private information without permission;
- deliberately damage school equipment, files or systems;
- download or install apps, software or browser extensions unless I have permission;
- try to bypass or interfere with the school's filtering, monitoring or security systems; or
- use school technology for something I know is illegal, unsafe or against school rules.

Using Artificial Intelligence (AI)

AI tools can help us to explore ideas, ask questions, create things and learn in new ways. They can also make mistakes, give incorrect information or produce things that are inappropriate.

When using AI for schoolwork:

- I will only use it when my teacher says that I may;
- I will follow my teacher's instructions about how it should be used;
- I will **think about and check** the information AI gives me rather than automatically believing it;
- I will not enter private or personal information about myself or anybody else;
- I will use AI to **help me think and learn**, not simply to do my work for me;
- I will be honest about using AI when my teacher asks me to explain how I completed my work; and
- I will tell an adult if an AI tool produces something that worries, upsets or confuses me.

If my teacher asks me to complete a piece of work independently, I will not use AI to create the work and pretend that I made it myself.

If something goes wrong

Sometimes people make mistakes when using technology. I might click the wrong link, send something to the wrong person or see something online that I did not mean to see.

If this happens, I will tell a trusted adult as soon as I can.

I understand that telling somebody about an honest mistake or something that worries me is the **right thing to do**.

I also understand that deliberately misusing technology or repeatedly ignoring these rules may have consequences in accordance with the school's Behaviour Policy.

My agreement

I have read and discussed this agreement and understand what Belmont Primary School expects of me when I use technology.

I will try to use technology in a way that is **safe, kind, responsible and honest**.

Pupil's name: _____

Pupil's signature: _____

Class: _____

Date: _____

Parent/Carer

I have discussed this agreement with my child and will support Belmont Primary School's approach to the safe, responsible and appropriate use of digital technology.

Parent/Carer's name: _____

Signature: _____

Date: _____