# Acceptable Use of ICT, Online Services and Digital Technology Policy

**Our vision:** Templars, a place where everyone belongs. A place where everyone is proud to belong. A school where everyone is welcomed, feels safe and strives to achieve their full potential.
**Our mission:** Every child, Every day, Every chance.
**Our values:** Care, Respect and Honesty.

Document Control
**Policy Owner:** Headteacher
**Approved by:** Headteacher
**Date Approved:** Autumn 2026
**Review Cycle:** Annually
**Next Review Due:** Autumn 2027, or earlier following relevant changes to legislation, guidance, technology or identified risk.

Distribution
- Available from the school office on request
- Shared with staff on SharePoint

**Safeguarding**

**At Templars Primary School, safeguarding and child protection are paramount. Safeguarding is the responsibility of every adult in our school community and applies equally to pupils' experiences online and offline.**

**Digital technology provides significant opportunities for teaching, learning, communication and inclusion. It can also expose children and adults to safeguarding, data protection and cyber security risks. The school therefore expects all users of its ICT systems, devices, online services and digital technology to use them safely, responsibly, professionally and lawfully.**

**All staff must remain alert to online safeguarding concerns and understand their responsibilities in relation to the school's filtering and monitoring arrangements. Staff must not deliberately bypass, disable or interfere with safeguarding or security controls and must report concerns about harmful or inappropriate online content, filtering or monitoring, digital communications or the use of technology in accordance with the school's safeguarding procedures.**

**Any concern relating to the safety or welfare of a child must be reported immediately in accordance with the school's Child Protection and Safeguarding Policy. Concerns about the conduct of an adult must be reported in accordance with the Staff Code of Conduct, Low-Level Concerns Policy and procedures for managing allegations against adults working with children.**

**Purpose**

Digital technology is an important part of teaching, learning, communication and the effective operation of Templars Primary School. Everyone who uses the school's ICT systems, devices, online services or digital technology has a responsibility to do so safely, securely, professionally and appropriately.

The purpose of this policy is to:

- establish clear expectations for the safe, responsible and lawful use of the school's ICT systems, devices, networks, online services and digital technology;
- safeguard pupils and adults when using technology;
- protect the confidentiality, integrity and security of school information and personal data;
- reduce the risk of cyber incidents, data breaches, misuse and unauthorised access;
- ensure users understand their responsibilities in relation to online safety, filtering and monitoring and cyber security;
- establish expectations for the responsible use of emerging technologies, including generative artificial intelligence (AI);
- protect the school's digital infrastructure, resources and reputation; and
- ensure that concerns, incidents and suspected breaches are identified, reported and responded to promptly.

This policy should be read alongside the school's Child Protection and Safeguarding Policy, Online Safety Policy, Data Protection Policy, Staff Code of Conduct, Behaviour Policy and other relevant policies and procedures.

---

**Summary Principles**

**Everyone using Templars Primary School's ICT systems, online services and digital technology must:**

**Safeguard**

- **Use technology in ways that protect the safety and welfare of children and adults.**
- **Follow the school's safeguarding, online safety, filtering and monitoring arrangements.**

- **Report safeguarding concerns or inappropriate online content promptly.**

**Secure**

- **Keep usernames, passwords and other authentication information secure.**
- **Never use another person's account or allow another person to use their account.**
- **Never deliberately bypass or interfere with security, filtering or monitoring controls.**

**Think Before Sharing**

- **Consider confidentiality, safeguarding, copyright and data protection before creating, uploading, storing, sharing or transmitting information.**
- **Use only school-approved systems and services for school information and personal data.**
- **Never enter confidential, sensitive or identifiable school information into an unapproved online service or generative AI tool.**

**Protect**

- **Take reasonable care of school equipment, systems and information.**
- **Protect personal, confidential and sensitive information.**
- **Report lost devices, suspected data breaches, phishing, malware or other cyber security concerns immediately.**

**Use Responsibly**

- **Use school systems, devices, online services and digital technology professionally, lawfully and appropriately.**
- **Only install, access or use software, applications, online services and AI tools that are permitted by the school.**
- **Do not create, access, store, share or transmit unlawful, harmful, discriminatory or otherwise inappropriate material.**

**Report**

- **If something goes wrong, report it promptly.**
- **Staff will not be criticised for reporting an accidental mistake or suspected cyber incident in good faith; early reporting enables the school to protect pupils, staff, systems and information.**

**Contents**

## 1 Scope

This policy applies to all staff, governors, volunteers, agency and supply staff, contractors and other authorised users of Templars Primary School's ICT systems, devices, networks, online services and digital technology.

For the purposes of this policy, these include:

- school-owned or managed computers, laptops, tablets, mobile devices and other digital equipment;
- school networks, internet access and wireless services;
- school email, Microsoft 365, SharePoint and other cloud-based services;
- management information, safeguarding, communication and curriculum systems;
- software, applications and online platforms provided or approved by the school;
- artificial intelligence (AI) and other emerging digital technologies used for school purposes;
- information and data created, accessed, processed, stored or transmitted using school systems; and
- access to school systems or information from outside the school premises, including remote access and authorised use of personal devices.

The expectations within this policy apply regardless of whether the user is working on or off the school premises.

Pupils' use of technology is additionally governed by the school's pupil acceptable use arrangements, Behaviour Policy and Online Safety Policy. The use of mobile phones, cameras and image-recording devices is addressed separately within the school's Mobile Phones, Cameras and Image-Recording Policy.

## 2 Governance and Responsibility

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

The Headteacher has operational responsibility for the implementation of this policy and may delegate specific responsibilities to appropriately trained members of staff.

The school will:

- comply with relevant legislation and statutory guidance relating to safeguarding, data protection, privacy, cyber security and the use of digital technology;
- maintain appropriate technical and organisational measures to protect its systems, users and information;
- ensure appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed at least annually;
- identify appropriate senior leadership, safeguarding and technical responsibilities for filtering and monitoring;

- provide staff with appropriate information, training and guidance so that they understand their responsibilities;
- maintain appropriate arrangements for responding to cyber incidents, data breaches and safeguarding concerns involving technology; and
- review this policy regularly and following significant changes to legislation, guidance, technology or identified risk.

All users must comply with this policy and with reasonable instructions issued by the Headteacher or another person acting with delegated authority.

Concerns about data protection should be referred to the school's Data Protection Officer. Safeguarding concerns must be reported in accordance with the school's Child Protection and Safeguarding Policy.

### 3 Intended Use

The school's ICT systems, devices, online services and digital technology are provided primarily to support the delivery of the school's vision and priorities, including teaching and learning, communication, administration and the safeguarding and welfare of pupils and staff.

Users are expected to use these resources responsibly, professionally, lawfully and in ways that support the work and values of Templars Primary School.

School systems and services must not be used in ways that compromise safeguarding, confidentiality, data protection, cyber security, the effective operation of the school or its reputation.

### 4 Personal Use

Limited personal use of school ICT facilities is permitted where this is reasonable, does not interfere with the user's work or the work of others, does not incur inappropriate cost and does not breach this or any other school policy.

Users must not:

- use school systems or equipment for unlawful, inappropriate or commercial purposes;
- store significant quantities of personal files, photographs or other personal information on school systems;
- use personal email, personal cloud storage or other unapproved personal accounts to store, send or process school information;
- use school systems in a way that could compromise safeguarding, confidentiality, security or the reputation of the school; or
- assume that personal use of school systems or devices is private.

Where personal devices are authorised to access school services, users must comply with the school's security, data protection and safeguarding requirements.

Professional boundaries in online communication and social media must be maintained at all times. Staff must not use personal accounts or private communication channels to establish or maintain relationships with pupils arising from their professional role. Further expectations are

set out in the Staff Code of Conduct, Online Safety Policy and Mobile Phones, Cameras and Image-Recording Policy.

### 5 Commercial and Financial Use

School ICT systems, devices, online services and digital resources must not be used for personal commercial activity, private business, personal financial gain or unauthorised fundraising.

This does not prevent authorised use undertaken legitimately on behalf of the school, including procurement, fundraising, lettings, partnership work or other approved school business.

Users must not use their school role, school systems, school data or access to the school community to promote or conduct private commercial activity without the prior authorisation of the Headteacher.

### 6 Identity, Passwords and Authentication

All users are responsible for protecting the accounts and credentials issued to them and for taking reasonable steps to prevent unauthorised access to school systems and information.

Users must:

- use secure passwords in accordance with the school's current password and cyber security requirements;
- keep usernames, passwords, PINs, authentication codes and other credentials confidential;
- use multi-factor authentication (MFA) where this is provided or required by the school;
- never share passwords or authentication codes with colleagues, pupils, family members or any other person;
- never use another person's account or allow another person to use their account, even where permission has been given;
- never approve an unexpected MFA request or authentication notification;
- lock their device whenever it is left unattended;
- ensure devices are secured against unauthorised access;
- take care that confidential or personal information displayed on screens, interactive boards or projectors cannot be viewed by people who should not have access to it; and
- immediately report any suspected compromise, unauthorised access or unexpected activity involving their account.

Users must not respond to unexpected or unsolicited requests for passwords, authentication codes or other security information. Suspicious emails, messages, links, QR codes, login pages or authentication requests must be treated with caution and reported in accordance with the school's cyber security procedures.

Where a user believes that their password or account may have been compromised, they must report this immediately and change their password as soon as it is safe and practicable to do so.

School devices will be configured, where technically appropriate, to lock automatically following a period of inactivity. Users remain responsible for manually locking devices whenever they leave them unattended.

Users must not impersonate another person, disguise their identity, attempt to gain unauthorised access to another person's account or deliberately circumvent authentication or security controls.

**7 Systems, Software and Cyber Security**

The school maintains technical and organisational measures to protect its digital systems, devices, networks and information. All users have a responsibility to support these measures and must not deliberately or negligently compromise the security or effective operation of school technology.

Users must only access systems, software, applications, online services and digital resources that they are authorised to use.

Users must not:

- damage, tamper with or deliberately misuse school ICT equipment, networks or systems;
- install, download or use unauthorised software, applications, browser extensions, plug-ins or other digital services;
- connect unauthorised devices, storage media or equipment to school systems or networks;
- alter device, browser, network or security settings without authorisation;
- disable, bypass or interfere with anti-malware, firewall, filtering, monitoring or other security controls;
- attempt to gain unauthorised access to systems, accounts, files, network equipment or information;
- establish unauthorised networks, servers, wireless access points or other services;
- deliberately, negligently or recklessly introduce malware or other harmful software;
- use school systems to undertake unauthorised scanning, testing or monitoring of networks or devices;
- transfer school information or personal data to an unauthorised system, application, online service or third-party provider; or
- use technology in any way that creates an unreasonable risk to the security, availability or integrity of school systems or information.

Software, applications, cloud services and other digital tools used for school purposes must be appropriately licensed, supported and approved in accordance with the school's procedures.

Users must not independently sign up to or introduce an online service, application or digital platform for processing school personal data without appropriate approval. Where a new service will process personal data, the school's data protection and procurement requirements must be followed before it is used.

Security updates, patches and other protective measures must not be prevented, disabled or deliberately delayed. School devices should be restarted or shut down when requested to allow security updates and maintenance to take effect.

Any suspected cyber security incident, malware infection, unauthorised access, unusual system behaviour or security weakness must be reported promptly to the appropriate member of staff or IT support. Where the incident may involve personal data or safeguarding, the Data Protection Officer and/or Designated Safeguarding Lead must also be informed as appropriate.

### 8 Equipment Care and Security

Users are expected to take reasonable care of school-owned or school-managed devices and equipment and to protect both the equipment and the information accessible through it.

Users must:

- take reasonable precautions to protect devices from loss, theft, accidental damage and unauthorised access;
- keep school devices secure when they are not in use;
- not leave laptops, tablets, mobile devices or other portable equipment unattended in public places or visible in unattended vehicles;
- not leave school devices in vehicles overnight;
- lock devices whenever they are left unattended;
- follow school instructions regarding the storage, charging, transport and use of equipment;
- not move, alter, repair, reconfigure or dispose of school equipment without appropriate authorisation;
- allow required security updates, maintenance and software installations to take place; and
- restart or shut down devices when requested or where necessary to enable security updates and maintenance.

Lost, stolen or potentially compromised devices must be reported **immediately** to the appropriate member of staff and IT support so that action can be taken to protect school systems and information. This may include disabling accounts, restricting access or remotely securing or wiping a device where technically possible.

Where the loss, theft or compromise of a device may involve personal data, the Data Protection Officer must also be informed without undue delay so that the school can assess whether a personal data breach has occurred.

School equipment remains the property of the school and must be returned when requested, when it is no longer required for the user's role or when the user's employment or other relationship with the school ends.

### 9 Information, Data Protection and Confidentiality

All users have a responsibility to protect the personal, confidential and sensitive information that they access, create, receive, store or share through their work.

Personal data must be handled in accordance with UK data protection legislation, the school's Data Protection Policy, Privacy Notices and associated procedures.

Users must:

- only access personal or confidential information where this is necessary and appropriate for their role;
- only use personal data for authorised school purposes and in accordance with the purpose for which it was obtained;
- use school-approved systems, applications and storage locations when creating, accessing, processing, storing or sharing school information;
- take particular care when handling special category, safeguarding or otherwise sensitive information;
- share personal or confidential information only with people who are authorised to receive it and only where there is an appropriate reason for doing so;
- ensure that only the minimum information necessary for the intended purpose is shared;
- check recipients, attachments, sharing permissions and access settings carefully before sending or sharing information;
- take reasonable steps to prevent personal or confidential information being seen, overheard or accessed by unauthorised people;
- follow the school's retention and secure disposal arrangements for digital information; and
- return or appropriately transfer school information and equipment when leaving employment or when it is no longer required.

School personal data must not be transferred to, stored within or processed using personal email accounts, personal cloud storage, unauthorised applications, online services or other unapproved systems.

Users must not access, alter, delete, copy, disclose or share personal or confidential information without appropriate authority or a lawful reason for doing so.

Data Breaches and Accidental Disclosure

Any actual or suspected loss, unauthorised disclosure, inappropriate sharing or unauthorised access to personal data must be reported immediately in accordance with the school's data breach procedures.

This includes, for example:

- sending an email or attachment to the wrong recipient;
- sharing a file or folder with inappropriate permissions;
- losing a device or document containing personal information;
- accidentally displaying confidential information to pupils or other unauthorised people;

- entering school personal data into an unauthorised online service or application; or
- becoming aware that someone may have accessed information without authorisation.

Users must report suspected breaches promptly even where they are unsure whether a breach has occurred. The Data Protection Officer will determine what further action, if any, is required.

Copyright and Intellectual Property

Users must respect copyright, licensing and intellectual property rights when creating, downloading, copying, adapting, storing or sharing digital material.

Software, images, text, video, music and other digital resources must only be used in accordance with applicable licences, permissions and copyright requirements.

## 10 Remote Working and Use of Personal Devices

School systems and information may be accessed remotely where this is necessary for school business and where the method of access has been approved by the school.

When working remotely, users remain subject to the same safeguarding, confidentiality, data protection and cyber security expectations that apply when working on the school premises.

Users must:

- access school systems and information only through approved services, applications and methods;
- ensure that devices used to access school systems are appropriately secured with password, PIN, biometric protection or other approved authentication;
- use multi-factor authentication where this is provided or required;
- lock devices whenever they are left unattended;
- take reasonable precautions to prevent confidential or personal information being seen, overheard or accessed by other people;
- avoid accessing sensitive information in public places where screens or conversations may be observed;
- take particular care when using public or shared networks and follow any school instructions relating to secure remote access;
- ensure that school information is stored within approved school systems rather than locally on a personal device wherever possible; and
- report the loss, theft, compromise or unauthorised access of any device used to access school systems promptly.

**Personal Devices**

Personal devices may only be used to access school systems or conduct school business where this is permitted by the school.

Where personal devices are used, users must:

- use only approved applications and services to access school information;

- ensure that the device has appropriate security protections and is kept up to date;
- prevent other people, including family members, from accessing school accounts, information or applications;
- not deliberately download or permanently store school personal data on the device unless specifically authorised;
- not transfer school information into personal email accounts, personal cloud storage, messaging services or other unapproved applications;
- log out of school systems where appropriate and ensure that access is protected when the device is not in use; and
- cooperate with reasonable action required by the school to protect school information where a personal device used for school business is lost, stolen or compromised.

The use of personal mobile phones, cameras and other image-recording devices in relation to pupils is governed by the school's Mobile Phones, Cameras and Image-Recording Policy.

**Paper Records When Working Remotely**

Where paper records containing personal or confidential information are taken away from the school premises for an authorised purpose, users must keep them secure, prevent access by unauthorised people and return them to school as soon as reasonably practicable.

Confidential or personal information must not be left unattended or visible in vehicles or other insecure locations.

## 11 International Access and Travel

Users must obtain prior approval before taking school-owned ICT equipment outside the United Kingdom or accessing school systems from overseas where this is not part of an authorised school activity.

Additional security measures or restrictions may be applied where necessary to protect school systems and information. Access from particular countries or locations may be restricted or blocked on security grounds.

Users travelling internationally must follow any additional instructions provided by the school, IT support or the Data Protection Officer regarding the security of devices, accounts and school information.

## 12 Email, Communication and Online Services

School-provided email, messaging, collaboration platforms and other online communication services must be used responsibly, professionally and securely.

School business should be conducted through school-approved accounts, systems and communication channels. Personal email accounts, personal messaging services, personal cloud storage or other unapproved communication platforms must not be used to send, receive, store or share school personal data or confidential information.

**Sending and Sharing Information**

Users must take particular care when sending or sharing information electronically.

Before sending an email, message, attachment or sharing link, users should:

- check that the intended recipients are correct;
- consider whether all recipients need to receive the information;
- check attachments and links before sending;
- use BCC where appropriate when communicating with groups of recipients whose email addresses should not be disclosed to one another;
- check access and sharing permissions when sending links to files or folders; and
- take additional care where the communication contains personal, confidential, safeguarding or otherwise sensitive information.

Where information is particularly sensitive, users should consider whether email or the proposed communication method is appropriate and use an approved more secure method where required.

School email must not be automatically forwarded to a personal or other unauthorised email account.

**Professional Communication**

Communication through school systems must reflect the same professional standards expected in face-to-face communication.

Users must not use school communication systems to create, send, forward or share material that is unlawful, abusive, threatening, discriminatory, harassing, defamatory or otherwise inappropriate.

Staff must maintain appropriate professional boundaries when communicating with pupils and families and must use school-approved communication channels for this purpose.

Users should be mindful that emails, messages and other digital communications created or received in the course of school business may form part of the school's official records and may be subject to disclosure in accordance with legal requirements.

**Suspicious Communications**

Users must exercise caution when receiving unexpected emails, messages, attachments, links, QR codes or requests for information.

Users must not provide passwords, authentication codes or other security credentials in response to unsolicited communications.

Suspected phishing, fraudulent or malicious communications should be reported promptly through the school's agreed procedures. Where a user has clicked a suspicious link, opened an unexpected attachment, provided information or approved an unexpected authentication request, this must be reported immediately so that protective action can be taken.

Users should not attempt to conceal an accidental error or suspected security incident.

## 13 Filtering and Monitoring

Templars Primary School recognises that safeguarding pupils includes protecting them from harmful and inappropriate content and activity online. The school maintains appropriate filtering and monitoring arrangements as part of its wider safeguarding responsibilities.

Filtering and monitoring work together but have different purposes:

- filtering helps prevent access to illegal, harmful or inappropriate online content; and
- monitoring helps identify potentially harmful or concerning online activity so that appropriate action can be taken.

No filtering or monitoring system can remove all online risk. Technical systems therefore support, rather than replace, effective staff supervision, professional judgement, safeguarding practice and the teaching of online safety.

**Responsibilities**

The Governing Body has overall strategic responsibility for ensuring that appropriate filtering and monitoring arrangements are in place.

The school will identify a responsible member of the Senior Leadership Team and a responsible governor for filtering and monitoring. The Designated Safeguarding Lead, Senior Leadership Team and IT support will work together to ensure that arrangements meet the safeguarding needs of the school.

The school will ensure that:

- appropriate filtering is applied to school networks, school-managed devices and other relevant internet access;
- monitoring arrangements reflect the age, needs and risk profile of pupils;
- filtering and monitoring arrangements do not unreasonably restrict teaching and learning;
- safeguarding and technical concerns arising from filtering and monitoring are appropriately reviewed and acted upon;
- staff understand their responsibilities and how to report concerns; and
- filtering and monitoring provision is reviewed at least once every academic year and additionally where significant safeguarding, technological or operational changes make this necessary.

The review will consider the school's context and pupil risk profile, including age, SEND, EAL, safeguarding needs, the ways in which technology is used and emerging risks and technologies, including generative AI.

**Staff Responsibilities**

All staff have a responsibility to support effective filtering and monitoring.

Staff must:

- provide appropriate supervision when pupils are using digital devices and online services;

- remain aware of how pupils are using technology during lessons and other school activities;
- not deliberately disable, bypass or attempt to circumvent filtering or monitoring controls;
- report where harmful, inappropriate or unsuitable material has been accessed or appears to be accessible;
- report suspected failures, weaknesses or misuse of filtering or monitoring systems;
- report where filtering unreasonably prevents legitimate teaching, learning or school business so that this can be reviewed appropriately;
- inform the appropriate person where planned teaching may reasonably generate unusual or potentially concerning filtering or monitoring activity; and
- report any safeguarding concern arising from online activity immediately in accordance with the school's safeguarding procedures.

Where monitoring identifies activity that may indicate a safeguarding concern, this will be considered and responded to in accordance with the school's Child Protection and Safeguarding Policy.

**Monitoring and Privacy**

Users of school systems and devices should understand that appropriate filtering and monitoring arrangements are in place and that activity on school networks, systems and school-managed devices may be monitored and recorded for safeguarding, security, operational and compliance purposes.

Monitoring will be undertaken lawfully, proportionately and in accordance with the school's data protection responsibilities and relevant privacy information.

## 14 Online Safety and Harmful or Inappropriate Content

Templars Primary School recognises that technology is a significant component of many safeguarding and wellbeing issues and that children may experience harm online as well as face to face. Online and offline safeguarding concerns may occur together and should not be considered in isolation.

The school considers online safety through the four broad areas of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation and content generated or manipulated using artificial intelligence;
- **Contact** – being subjected to harmful online interaction with other users, including peer pressure, commercial advertising and adults posing as children or young people with the intention of grooming or exploiting them;
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, including making, sending or receiving explicit images, online bullying, harassment and sharing other people's personal information without consent; and

- **Commerce** – risks arising from online commercial activity, including inappropriate advertising, scams, phishing, financial exploitation and gambling-related content.

**Expectations for Users**

Users must not use school systems, devices, networks or online services to deliberately create, access, download, store, send, post or share material that is illegal or that could reasonably be considered harmful, abusive, threatening, discriminatory, hateful, sexually inappropriate or otherwise unsuitable for a school environment.

Users must not use school technology to bully, intimidate, harass, exploit, impersonate or deliberately cause harm to another person.

The deliberate creation, possession, viewing or sharing of illegal content will be treated seriously and may be referred to the police or other appropriate agencies.

**Safeguarding Concerns**

Where a user encounters harmful, inappropriate or concerning online material unintentionally, they should not deliberately continue to access, copy, download or share it.

Staff must report:

- online activity or content that raises a concern about the safety or welfare of a pupil;
- harmful or inappropriate material that is accessible through school systems;
- concerning online communication involving a pupil;
- suspected online bullying, harassment, grooming, exploitation, radicalisation or other harmful behaviour;
- concerns relating to the creation or sharing of nude or semi-nude images;
- online behaviour that may constitute child-on-child abuse; and
- any other online activity that may indicate that a child is at risk of harm.

Safeguarding concerns must be reported promptly in accordance with the school's Child Protection and Safeguarding Policy. Staff must not undertake their own investigation or unnecessarily view, copy, print, save or forward harmful or illegal material.

Where there is uncertainty about whether online content or activity constitutes a safeguarding concern, staff should seek advice from the Designated Safeguarding Lead or a Deputy Designated Safeguarding Lead.

**Education and Supervision**

The school will support pupils to develop the knowledge, skills and judgement needed to use technology safely and responsibly.

Staff supervising pupils using technology must maintain appropriate awareness of pupils' online activity and reinforce the school's expectations for safe and responsible use.

Filtering and monitoring systems support this work but do not replace appropriate supervision, professional curiosity or safeguarding practice.

## 15 Generative Artificial Intelligence (AI) and Emerging Technology

Templars Primary School recognises that generative artificial intelligence (AI) and other emerging technologies can support teaching, learning, accessibility, administration and staff workload when used appropriately.

The use of AI does not remove or reduce the professional responsibility of the person using it. Staff remain accountable for the accuracy, appropriateness, quality and consequences of work produced or supported by AI.

**Approved Use**

Staff may use generative AI and other emerging technologies for school purposes where the tool and proposed use are permitted by the school.

AI may be used to support appropriate professional tasks such as generating ideas, developing resources, adapting materials, supporting planning, drafting communications and reducing administrative workload.

Users must not independently introduce an AI service for processing school personal data or for pupil use without appropriate school approval.

**Data Protection and Confidentiality**

Users must protect personal, confidential and sensitive information when using AI.

Unless the school has specifically approved the tool and its use for the information concerned, users must not enter, upload or disclose:

- identifiable pupil, parent, carer or staff information;
- safeguarding information;
- special category or other sensitive personal data;
- confidential school information;
- information relating to individual behaviour, attainment, attendance, SEND, medical needs or family circumstances; or
- documents, photographs, recordings or other material containing identifiable personal information.

Information must not be assumed to be anonymous simply because a person's name has been removed. Users should consider whether an individual could still reasonably be identified from the information provided.

Where the use of an AI tool involves personal data, the school's data protection requirements must be followed and advice sought from the Data Protection Officer where necessary.

**Accuracy and Professional Judgement**

AI-generated information may be inaccurate, incomplete, biased, outdated or misleading.

Staff must:

- critically review and fact-check AI-generated content before relying upon or sharing it;

- ensure that material is appropriate for the age, needs and circumstances of the intended audience;
- check for bias, stereotyping, discriminatory content or other inappropriate assumptions;
- exercise their own professional judgement rather than treating an AI-generated response as authoritative; and
- take responsibility for the final content or decision.

AI must not be used as a substitute for professional judgement in safeguarding, SEND, behaviour, assessment or other decisions concerning individual pupils.

**Safeguarding**

AI must be used in accordance with the school's safeguarding and online safety arrangements.

Any AI-generated content, interaction or pupil use that raises a safeguarding concern must be reported in accordance with the school's Child Protection and Safeguarding Policy.

Staff must not use AI to generate, manipulate or alter content in a way that is harmful, deceptive, discriminatory, sexually inappropriate or otherwise inconsistent with the school's safeguarding responsibilities and professional standards.

**Pupil Use**

Pupils may only use generative AI through tools, accounts and activities that have been approved by the school and under an appropriate level of staff direction and supervision.

Any pupil-facing AI tool must be considered for suitability, including the age and needs of pupils, safeguarding arrangements, filtering and monitoring, privacy, data protection and the educational purpose of its use.

Pupils should be taught to understand that AI-generated information may be inaccurate or misleading and to use AI critically, safely and responsibly.

**Intellectual Property and Transparency**

Users must respect copyright, intellectual property and licensing requirements when entering material into AI tools or using AI-generated outputs.

Copyrighted, confidential or proprietary material must not be uploaded to an AI service where the user does not have appropriate authority or permission to do so.

Where appropriate, users should be transparent about significant use of generative AI in their work and must not present AI-generated material in a misleading way.

**Emerging Technology**

The same principles of safeguarding, professional accountability, data protection, security, transparency and responsible use apply to new and emerging digital technologies not specifically named within this policy.

Where a user is uncertain whether a technology, tool or proposed use is permitted, they should seek advice before using it for school purposes.

## 16 Malware, Phishing and Cyber security Incidents

All users have a responsibility to help protect the school from cyber security threats and to report suspected incidents promptly.

Users should remain alert to phishing, malware, ransomware, fraudulent communications, impersonation and other attempts to gain unauthorised access to school systems, accounts, information or finances.

**Preventing Cyber Incidents**

Users must:

- exercise caution when opening unexpected or unusual emails, messages, attachments, links or QR codes;
- check unexpected requests for information, payments, password resets or changes to financial details through an appropriate alternative method;
- not provide passwords, authentication codes or other security credentials in response to unsolicited requests;
- only download software, applications or files from approved or trusted sources;
- not deliberately disable or interfere with anti-malware, firewall or other security protections;
- follow school instructions and training relating to cyber security; and
- report suspicious communications, activity or system behaviour promptly.

**Reporting a Suspected Incident**

Users must immediately report any actual or suspected cyber security incident, including where they:

- click a suspicious or unexpected link;
- open a suspicious attachment;
- provide information in response to a suspected phishing or fraudulent communication;
- approve an unexpected authentication request;
- suspect that an account or password has been compromised;
- notice unusual activity on an account, device or school system;
- become aware of malware, ransomware or another security threat;
- lose a device used to access school systems or information; or
- become aware of unauthorised access to school systems or data.

Users should report concerns even where they are uncertain whether a cyber incident has occurred.

Prompt reporting enables the school and its IT support to contain potential threats, protect information and systems and determine whether further safeguarding, data protection or external reporting action is required.

Staff should not attempt to conceal an error or suspected incident. A user who reports an accidental mistake or suspected cyber security incident promptly and in good faith enables the school to take appropriate protective action.

**School Response**

Suspected cyber security incidents will be referred to the appropriate school leader and IT support and managed in accordance with the school's cyber incident response and business continuity arrangements.

Where appropriate, the Data Protection Officer, Designated Safeguarding Lead, Headteacher and Governing Body will be involved.

The school will determine whether an incident requires reporting to relevant external organisations, regulatory bodies, law enforcement, insurers or other agencies.

## 17 Removable Media

The use of USB memory sticks and other removable storage devices is not permitted on school ICT systems or for school business.

Users must not:

- connect USB memory sticks, portable storage devices or other removable storage media to school-owned or school-managed devices;
- use personal removable storage devices to store, transfer or process school information; or
- copy school information onto removable storage media.

School information and files must be stored and shared using school-approved systems and services, such as the school's approved Microsoft 365, OneDrive and SharePoint environment.

Any removable storage device found to contain school personal, confidential or sensitive information must not be accessed or transferred further and must be reported promptly to the appropriate member of staff or IT support.

## 18 Monitoring and Access to School Systems

The school may monitor, record and review the use of its ICT systems, networks, devices and online services where this is necessary and appropriate for safeguarding, cyber security, system administration, business continuity, compliance with school policies, investigation of concerns or fulfilment of legal obligations.

Users should not assume that activity undertaken using school accounts, systems, networks or school-managed devices is private.

Monitoring or review may include, where appropriate:

- internet and network activity;
- access and authentication records;
- system and security logs;
- school email and communication systems;
- files and information stored within school-managed systems;
- use of school-provided applications and online services; and
- activity identified through the school's filtering and monitoring arrangements.

Any monitoring or access will be undertaken lawfully, fairly and proportionately and in accordance with the school's data protection responsibilities, privacy information and relevant policies.

Access to an individual user's account, email, files or other information will only take place where there is an appropriate reason and appropriate authorisation.

The school may access school accounts, files or communications where this is reasonably necessary to:

- safeguard a child or adult;
- investigate a safeguarding, conduct, security or data protection concern;
- respond to a cyber security incident;
- maintain essential school operations or business continuity;
- locate or recover school records or information;
- respond to a lawful request for information; or
- meet another legal or regulatory obligation.

Where appropriate, access will be authorised by the Headteacher or another suitably authorised senior leader and will be undertaken with appropriate technical, data protection or safeguarding advice.

Information obtained through monitoring or authorised access will only be used for legitimate purposes and will be shared only where there is an appropriate reason to do so.

### 19 Information Storage, Records and Business Continuity

School information and records must be stored within appropriate school-approved systems and locations so that they remain secure, accessible and available for legitimate school purposes.

Documents and records required by colleagues or necessary for the ongoing operation of the school should be stored in the appropriate shared school location, such as an authorised SharePoint area, rather than being held solely within an individual's email account, OneDrive or device.

Users must:

- follow the school's agreed arrangements for storing, organising and sharing information;
- use appropriate shared locations for records that form part of the school's corporate or operational information;
- avoid creating unnecessary duplicate copies of personal or confidential information;
- follow the school's retention and deletion requirements;
- not deliberately delete, remove or withhold school records that the school is required to retain; and
- ensure that school information for which they are responsible is appropriately transferred or made accessible when changing role or leaving the school.

The school may take authorised and proportionate steps to access or recover school information where this is necessary for safeguarding, legal compliance, business continuity or the effective operation of the school.

### 20 Reporting Concerns, Incidents and Breaches

Users must report concerns, incidents and suspected breaches promptly so that appropriate action can be taken to protect pupils, staff, information and school systems.

This includes:

- safeguarding concerns involving technology or online activity;
- harmful or inappropriate online content;
- concerns about filtering or monitoring;
- suspected phishing, malware or other cyber security incidents;
- compromised accounts, passwords or authentication;
- lost or stolen devices;
- actual or suspected personal data breaches;
- unauthorised access to school systems or information;
- accidental disclosure or inappropriate sharing of information;
- misuse of school technology; and
- suspected breaches of this policy.

**Who to Report To**

**Safeguarding concerns** must be reported immediately to the Designated Safeguarding Lead or a Deputy Designated Safeguarding Lead in accordance with the school's safeguarding procedures.

**Cyber security or technical concerns** must be reported promptly to the school's IT support and/or the appropriate responsible member of staff.

**Actual or suspected personal data breaches** must be reported promptly to the Data Protection Officer or through the school's agreed data breach reporting arrangements.

**Concerns about the conduct of an adult** must be reported in accordance with the school's procedures for allegations and low-level concerns.

Where a concern falls into more than one category, users should not delay reporting while deciding which procedure applies. The school will ensure that the concern is referred to the appropriate people.

Users are expected to report accidental mistakes and suspected incidents promptly and in good faith. Early reporting allows the school to reduce potential harm and take appropriate action.

## 21 Breaches, Sanctions and Disciplinary Action

All users are expected to comply with this policy and with reasonable instructions relating to the safe and secure use of school technology.

Suspected breaches of this policy will be considered appropriately and proportionately, taking account of the nature and seriousness of the incident, the circumstances in which it occurred, any potential or actual harm, whether the action was deliberate or reckless, and how promptly the matter was reported.

Where appropriate, the school may:

- provide advice, support, additional training or guidance;
- require changes to working practices;
- restrict, suspend or remove access to particular systems, services, devices or accounts;
- take action in accordance with the school's disciplinary or other relevant procedures;
- investigate the matter under safeguarding, data protection, cyber security or staff conduct procedures; and
- refer the matter to an appropriate external organisation or authority where required.

Deliberate, reckless, repeated or serious misuse of school ICT systems, digital technology, personal data or online services may constitute misconduct and may result in disciplinary action.

Where there is reason to believe that a criminal offence may have been committed, the school will consider whether the matter should be referred to the police or another appropriate authority.

Nothing within this section prevents the school from taking immediate action where this is necessary to safeguard a child or adult, protect personal data, secure school systems or prevent further harm.

**Reporting Mistakes and Incidents**

The school recognises the importance of a culture in which users feel able to report mistakes, concerns and suspected incidents promptly.

An accidental error that is reported promptly and in good faith will be considered differently from deliberate misuse, reckless behaviour, repeated failure to follow reasonable instructions or an attempt to conceal an incident.

Users must therefore report mistakes and suspected breaches as soon as possible so that the school can take appropriate action to reduce risk and prevent further harm.

## 22 Related Policies, Legislation and Guidance

This policy should be read alongside relevant school policies and procedures, including:

- Child Protection and Safeguarding Policy
- Online Safety Policy
- Staff Code of Conduct
- Data Protection Policy and Privacy Notices
- Behaviour Policy
- Mobile Phones, Cameras and Image-Recording Policy
- Low-Level Concerns Policy
- Procedures for Managing Allegations Against Staff and Volunteers
- Cyber security and Business Continuity arrangements
- Records Management and Retention arrangements
- SEND Policy
- Equality Policy

**Legislation and Statutory Guidance**

The school will have regard, where relevant, to current legislation and statutory guidance, including:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Equality Act 2010
- Human Rights Act 1998

- Education Act 2011
- Keeping Children Safe in Education 2026

**Department for Education and Other National Guidance**

The school will also have regard to relevant current guidance and standards, including:

- DfE *Filtering and Monitoring Standards for Schools and Colleges*
- DfE *Cyber Security Standards for Schools and Colleges*
- DfE digital and technology standards for schools and colleges
- DfE guidance on data protection in schools
- DfE guidance and standards relating to generative artificial intelligence in education
- DfE guidance on mobile phones in schools
- Information Commissioner's Office guidance on data protection, information security and monitoring in the workplace

This policy will be reviewed regularly and updated where necessary in response to changes in legislation, statutory guidance, national standards, technology, identified risks or school practice.