Caister Primary Federation

Staff, Guest and Governor Acceptable Use Policy

Formally adopted by the Governing Board of:-	**Caister Primary Federation**
On:-	**January 2026**
Chair of Governors:-	**Payal Patel**
Last updated:-	**May 2022**

Table of Contents

Table of Contents 2
Policy Introduction 3
Social Media 5
Managing digital content 5
Learning and teaching 6
Email 6
Mobile phones and devices 6
General acceptable use requirements for WhatsApp 7
Use of WhatsApp by leaders for operational matters 7
Staff use of WhatsApp for reporting illness 7
Use of mobile phones during off-site visits 8
Use of mobile phones within the SRB environment. 8
Appendix 1 – Table of changes 9
Agreement 10

Policy Introduction

This document has been developed to ensure staff within Caister Primary Federation are aware of their professional responsibilities when using the Federation's ICT equipment and systems. All staff will follow the guidelines at all times. You are responsible for your behaviour and actions when carrying out any activity which involves using ICT equipment and information systems, either within school or at other locations, such as home. ICT equipment includes all devices and authorised cloud services used to access the organisation's digital systems and internet resources, as well as standalone devices with digital storage.

I will comply with the following statements:

- I will access the internet and other ICT services using an individual username and password, which I will keep secure and private.
- I will never allow other users to access services via my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the ICT Coordinator, Network Manager or the Head of School.
- I will ensure that I use a suitably complex password for accessing and registering services, and that I use a unique password for each service. Where sensitive data is stored or accessed, I will always enable and use multifactor authentication.
- I will not share my passwords with any colleagues or pupils within school.
- I will seek consent from the ICT Coordinator, Network Manager or Head of School prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material, I will report it immediately to the ICT coordinator, Network Manager or Head of School.
- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform. If I identify or suspect any failure, weakness, or inappropriate content not being correctly filtered, I will immediately report this to the ICT Coordinator, Network Manager, or Head of School to ensure pupil safety and compliance with safeguarding expectations.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Coordinator, Network Manager.
- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.

- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.
- I will secure any equipment taken off site for school trips.
- I will only use school-owned or provided portable storage (USB sticks, portable hard drives etc) when storing on an approved cloud base system is not an option.
- I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/ password protection deployed.
- Any information asset that I create from other information systems, and which could be deemed personal or sensitive, will be stored within the school's approved cloud-based services *(e.g., Microsoft 365)*. Access will be appropriately controlled in accordance with the school's data-protection requirements*. (For example: spreadsheets or other documents created using data from the school information-management system.)*
- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard myself or others.
- I understand that if I do not follow all statements in this AUP and in other school policies relating to the use of ICT equipment I may be subject to disciplinary action in line with the schools established disciplinary procedures.

Social Media

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, X and YouTube or any other online publishing websites.
- I must not use social media tools to communicate with current or former pupils under the age of 18.
- I will not use any social media tools to communicate with parents unless approved in writing by the Head of School.
- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.
- Staff must not access social networking sites for personal use during working hours. Any social media accessed outside of this time, such as breaks, should not use the school Wi-Fi or Guest Network.
- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to the Network Manager or Head of School.

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
- I will only use AI platforms, tools, or services that have been approved by the school and are part of our authorised cloud environment. I will not use any AI platform that permits, promotes, or contains adult content, or that cannot guarantee appropriate safeguarding and data-protection standards.
- I will only use school equipment to create multimedia. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the E-Safety Policy.
- Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from the designated member of staff (Head of School or Executive Head of School).
- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright law.
- I will ensure that any images, videos, or sound recordings of pupils are stored securely within the organisation's authorised cloud environment and are not transferred to, or stored on, any personally-owned device.
- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Learning and teaching

- I will support and promote the school E-Safety policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.

Email

- I will communicate with colleagues only through approved internal platforms such as Microsoft Teams or my school email address. All communication with parents or external agencies will be conducted exclusively through my school email account. I will never use a personal email address for any school-related communication.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in subject folders.
- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

Mobile phones and devices

- I will ensure that my mobile phone and any other personally owned device is switched off or switched to ‘silent’ mode during school working hours.
- Bluetooth communication will be ‘hidden’ or switched off, and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team.
- During normal workday school hours, I will not contact any parents on my personally owned device.
- I will not contact any pupils on my personally owned device.
- I will not use any personally owned mobile device to take images, video or sound recordings.

General acceptable use requirements for WhatsApp

All use of WhatsApp by staff and leaders must comply with the organisation's wider Acceptable Use Policy, including:

- Maintaining the privacy and security of all organisational data.
- Ensuring that communication remains appropriate, lawful, and aligned with professional expectations.
- Avoiding the sharing, storing, or discussion of any information relating to children, families, or safeguarding matters.

Use of WhatsApp by leaders for operational matters

Leaders may use WhatsApp for internal communication strictly for operational purposes where this enables timely and effective coordination. The following controls must be adhered to:

- WhatsApp is to be used as a supplementary communication tool only, and not as the primary method for recording, storing, or managing operational decisions.
- No personal, confidential, or sensitive information relating to children, families, or staff may be shared on WhatsApp under any circumstances.
- Messages must be limited to routine operational updates, scheduling matters, and urgent notifications that do not contain personally identifiable information.
- Where operational decisions or actions need to be formally recorded, they must be documented within approved organisational systems (e.g., email, MIS, safeguarding software) at the earliest practicable opportunity.
- Leaders are responsible for ensuring that participation in WhatsApp groups is professional, respectful, and compliant with the organisation's Acceptable Use and Data Protection policies at all times.
- Use of WhatsApp must comply with the organisation's data protection, confidentiality, and record-keeping requirements; WhatsApp groups must be closed and deleted when no longer operationally necessary.

Staff use of WhatsApp for reporting illness

Staff may use WhatsApp to notify leaders of illness only where this has been agreed as part of the organisation's communication procedures and where this falls within the boundaries of the Acceptable Use Policy.

The following conditions apply:

- WhatsApp may be used solely for brief, factual notifications of absence (e.g., illness, delayed arrival), without sharing medical details or personal sensitive information.
- Staff must ensure that any absence message is directed to the designated contact person or group, in accordance with internal reporting procedures.
- WhatsApp must not be used to discuss colleagues' absences, health conditions, or any personal details of other staff members.

- All communication must remain professional in tone and content, in line with the Staff Code of Conduct.
- Staff must continue to complete any required HR or attendance documentation through the approved organisational systems.

Use of mobile phones during off-site visits

Staff supervising off-site visits, including residentials are permitted to carry their personal mobile phones on their person for the specific purpose of communicating with colleagues when this supports pupil safety, regulation, or operational needs.
The use of mobile phones in this incidence is subject to the following conditions:

- Mobile phones must remain on the staff member's person at all times and must not be left unattended or accessible to pupils.
- Phones must be used solely for professional communication with colleagues and not for personal use during working time.
- Any messaging used for communication must be set to auto-delete or disappear, ensuring no messages are stored on the device.
- Pupils' names or other identifying information must not be used in any message or communication.
- Phones must not be used to take photographs, videos, or audio recordings of pupils under any circumstances, unless explicitly authorised in line with school policy.
- All use must comply with the school's Safeguarding, GDPR, Staff Code of Conduct, and Mobile Phone policies.
- Where a personal mobile device is required to contact a parent or carer, the staff member must take all reasonable steps to withhold their number in the first instance. In circumstances where this is not feasible, or where a return call from the parent or carer is necessary, the parent/carer's number must be removed or blocked from the staff member's device at the earliest practicable opportunity following the conclusion of the incident.

This recognises the additional communication needs during off-site visits while maintaining the highest standards of safeguarding, confidentiality, and professional conduct.

Use of mobile phones within the SRB environment.

Staff working within the SRB (Specialist Resource Base) environment are permitted to carry their personal mobile phones on their person during the school day for the specific purpose of communicating with colleagues when this supports pupil safety, regulation, or operational needs.
The use of mobile phones in the SRB is subject to the following conditions:

- Mobile phones must remain on the staff member's person at all times and must not be left unattended or accessible to pupils.
- Phones must be used solely for professional communication with colleagues and not for personal use during working time.
- Any messaging used for communication must be set to auto-delete or disappear, ensuring no messages are stored on the device.
- Pupils' names or other identifying information must not be used in any message or communication.

- Phones must not be used to take photographs, videos, or audio recordings of pupils under any circumstances, unless explicitly authorised in line with school policy.
- All use must comply with the school's Safeguarding, GDPR, Staff Code of Conduct, and Mobile Phone policies.

This recognises the additional communication needs within the SRB environment while maintaining the highest standards of safeguarding, confidentiality, and professional conduct.

Appendix 1 – Table of changes

Date of change	Paragraphs affected	Summary of update
3/2/2026	Use of mobile phone for off-site visits	Added to document to clarify use of personal phones during off-site visits
	Use of WhatsApp	Added to document to clarify specific use of WhatsApp within work environment
09/01/2026	Whole Document	Added reference to Network Manager & updated Head Teacher to Head of School. Updated reference of School Network to modern cloud-based terminology.
09/01/2026	Policy Introduction	Added 'when using the Federation's ICT equipment and systems' to opening sentence.
09/01/2026	Policy Introduction point 3	Added reference to multifactor authentication
09/01/2026	Policy Introduction point 7	Updated the reporting of issues with the filtering platform
09/01/2026	Policy Introduction point 12	Added criteria that removable/portable storage devices should only be used when cloud storage is not available
09/01/2026	Managing Digital Content Point 2	Added bullet point concerning the use of AI platforms
09/01/2026	Email Point 1	Added reference to internal communication allowed via internal platforms such as MS Teams
26/01/2026	Page 9	Addendum added in relation to mobile phone use within the SRB environment

Agreement

I have read and understand all of the Caister Primary Federation Staff/Guest/Governor Acceptable Use Policy relating to my use of technology within school.

I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Staff name: _____

Signed: _____

Date: _____