Aiskew, Leeming Bar
Church of England Primary School

'Rooted in love and growing together
to become lifelong learners'

ACCEPTABLE
USE
POLICY

Date written: March 2022. Reviewed and reissued September 2022.

Date agreed and ratified by the Board of Governors: 28th March 2022

Signed: _____   Date: _____
(Headteacher)

Signed: _____   Date: _____
(on behalf of the Board of Governors)

Date of review: Spring 2024

Introduction

In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) became enforceable across the United Kingdom. As part of Aiskew, Leeming Bar CE Primary School's programme to comply with the new legislation it has written a new suite of Information Governance policies.

The Acceptable Use policy governs the use of the School's corporate network that individuals use on a daily basis in order to carry out business functions.

This policy should be read in conjunction with the other policies in the School's Information Governance policy framework.

Scope

All policies in Aiskew, Leeming Bar CE Primary School's Information Governance policy framework apply to all School employees, any authorised agents working on behalf of the School, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:
- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

Email and Instant Messaging Use

The School provides email accounts to employees to assist with performance of their duties. The School also allows employees to use its instant messaging service (via Teams). For the benefit of doubt Instant Messages are classed as email communications in this policy.

Personal Use
Whilst email accounts should primarily be used for business functions, incidental and occasional use of the email account in a personal capacity may be permitted so long as:
- Personal messages do not tarnish the reputation of the School,
- Employees understand that emails sent to and from corporate accounts are the property of the School,
- Employees understand that School management may have access to their email account and any personal messages contained within,

- Employees understand that the emails sent to/from their email account may have to be disclosed under Freedom of Information and/or Data Protection legislation,
- Employees understand that the School reserves the right to cleanse email accounts at regular intervals which could result in personal emails being erased from the corporate network,
- Use of corporate email accounts for personal use does not infringe on business functions.

Inappropriate Use

The School does not permit individuals to send, forward, or solicit emails that in any way may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit messages, images, cartoons, jokes or movie files,
- Unwelcome propositions,
- Profanity, obscenity, slander, or libel,
- Ethnic, religious, or racial slurs,
- Political beliefs or commentary,
- Any messages that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Other Business Use

Users are not permitted to use emails to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School management.

Email Security

Users will take care to use their email accounts in accordance with the School's information security policy. In particular users will:

- Not click on links in emails from un-trusted or unverified sources,
- Use secure email transmission methods when sending personal data,
- Not sign up to marketing material that could jeopardise the School's IT network,
- Not send excessively large email attachments without authorisation from School management and the School's IT provider.

Group Email Accounts

Individuals may also be permitted access to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to suspension of an individual's email rights. **Mrs Bethany Stanley** will have overall responsibility for allowing access to group email accounts but this responsibility may be devolved to other individuals.

The School may monitor and review all email traffic that comes to and from individual and group email accounts.

Internet Use

The School provides internet access to employees to assist with performance of their duties.

Personal Use

Whilst the internet should primarily be used for business functions, incidental and occasional use of the internet in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the School,
- Employees understand that School management may have access to their internet browsers and browsing history contained within,
- Employees understand that the School reserves the right to suspend internet access at any time,
- Use of the internet for personal use does not infringe on business functions.

Inappropriate Use

The School does not permit individuals use the internet in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic images, cartoons, jokes or movie files,
- Images, cartoons, jokes or movie files containing ethnic, religious, or racial slurs,
- Any content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Individuals are also not permitted to use the internet in a way which could affect usage for others. This means not streaming or downloading media files and not using the internet for playing online games.

Other Business Use

Users are not permitted to use the internet to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School management.

Internet Security

Users will take care to use the internet in accordance with the School's information security policy. In particular users will not click on links on un-trusted or unverified web pages.

Platforms for Online Learning and Communicating with Pupils

School uses Seesaw, Purple Mash and Microsoft Teams/Office 365 as methods of communicating with pupils. For Seesaw accounts, as least 2 staff members oversee a single account. James Hodgson (ICT lead) oversees all communication via Purple Mash. Microsoft Teams/Office 365 has been set up safely by Schoolsict. For staff recording themselves via these platforms must wear suitable clothing and try where possible (activity dependent) to just include their head or the object they are trying to

show e.g. whiteboard/counters etc. Any computers used should be in appropriate areas, for example, not in bedrooms. If live classes take place, these should be recorded so that if any issues were to arise, the video can be reviewed. Language must be professional and appropriate, including any family members in the background. Pupils too should be reminded about wearing suitable clothing and taking videos in appropriate areas e.g. not in bedrooms.

Social Media Use

The School recognises and embraces the benefits and opportunities that social media can contribute to an organisation. The School also recognises that the use of social media is a data protection risk due to its open nature and capacity to broadcast to a large amount of people in a short amount of time.

Corporate Accounts
The School has a number of social media accounts across multiple platforms, these include a closed Facebook page which primarily parents/carers use, in addition to other members of the school community. School also has its own Twitter account. Nominated employees will have access to these accounts and are permitted to post general information about the School. Authorised employees will be given the usernames and passwords to these accounts which must not be disclosed to any other individual within or external to the organisation. **Mrs Bethany Stanley** will have overall responsibility for allowing access to social media accounts. School also blogs from both classes. These blogs are found on the school website. There will never be the name of a child and his/her picture.

Corporate social media accounts must not be used for the dissemination of personal data either in an open forum or by direct message. This would be a contravention of the School's information governance policies and data protection legislation.

Corporate social media accounts must not be used in a way which could:
- Tarnish the reputation of the School,
- Be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.
- Be construed as sexually explicit,
- Construed as political beliefs or commentary.

Personal Accounts
The School understands that many employees will use or have access to personal social media accounts. Employees must not use these accounts:
- During working hours,
- Using corporate equipment,
- To conduct corporate business,
- To contact or approach clients, customers, or partners of the School.

Telephone and Video Conferencing Use

The School provides email accounts to employees to assist with performance of their duties. The School also allows employees to use Skype for Business, Microsoft Teams and Zoom. For the benefit of doubt Skype, Teams and Zoom calls are classed as telephone calls in this policy.

Personal Use

Whilst the telephone should primarily be used for business functions, incidental and occasional use of the telephone in a personal capacity may be permitted so long as:

- Usage does not tarnish the reputation of the School,
- Employees understand that School management may have access to call history,
- Employees understand that the School reserves the right to suspend telephone usage at any time,
- Use of the telephone for personal use does not infringe on business functions.

Inappropriate Use

The School does not permit individuals use the telephone in a way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

Other Business Use

Users are not permitted to use the telephone to carry out their own business or business of others. This includes, but not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case by case basis at the discretion of School management.

Appendix A

Acceptable Usage Policy – Staff – Linked to 360Safe AUP Guidelines

This document has been written to ensure that staff use the ICT throughout the school appropriately. If they have any questions regarding this policy, they should direct them to the Head Teacher or ICT Subject Leader.

Staff should:

- Use computers and equipment with care and ensure children do the same e.g. water bottles should stay away from machines
- Ensure that usernames and passwords are not shared with children or other staff
- Ensure that they log off when they have finished using a computer
- Make use of resources such as cameras and microphones but ensure that these are returned after their use. They should also endeavour to remove pictures/files on return too
- Try not to be wasteful, in particular when it comes to batteries, printer ink and paper
- Ensure that online dialogue (e.g. blog posts or emails) with other schools or parents remains professional at all times
- Ensure that online activity is related to their professional duty
- Ensure that they are not using the school's ICT for financial gain e.g. auction or betting sites
- Ensure that they have read and understood the E-safety Policy
- Be aware that software or hardware should not be installed without prior consent of the ICT Subject Leader or Head Teacher
- Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the Head Teacher
- Where data of a personal nature such as school reports, IEPs, correspondence, photographs and assessment data is taken home on a school laptop or other storage device, it must be recognised that this data comes under the GDPR Act 2018 and is subject to the school's Privacy Policy. Care must therefore be taken to ensure its integrity and security. It must not be transferred to home computers. Where staff are using their own digital equipment such as cameras and mobile phones, extreme caution is advised to avoid misinterpretation by others. The use of these for specific activities must be agreed with the headteacher beforehand.
  Files should be transferred to school equipment as soon as possible
- Report any issues to the Head Teacher or ICT Subject Leader as soon as possible
- Return any hardware or equipment if they are no longer employed by the school

Signed _____ Print _____

Date _____

Appendix B

Acceptable Usage Policy KS2 Children – Linked to 360Safe AUP Guidelines

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using the computers. When we talk about ICT, we are talking about computers, netbooks, iPads and everything else including cameras and other devices. By using the ICT
in school, you have agreed to follow these rules. These rules will be discussed with you as a class before you sign them. A copy of this will also be sent home to your parents. If you have any questions, please ask your teacher.

- At all times, I will think before I click (especially when deleting or printing)
- When using the Internet, I will think about the websites I am accessing
- If I find a website or image that is inappropriate, I will tell my teacher straight away
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site
- When communicating online (in blogs, email etc) I will think about the words that I use and will not use words that may offend other people
- When communicating online, I will only use my first name and not share personal details such as my email address my home address or my phone number
- I understand that people online might not be who they say they are
- I will not look at other people's files or documents without their permission
- I will not log on using another person's account
- I will think before deleting files
- I will think before I print
- I know that the teachers can, and will, check the files and websites I have used
- I will take care when using the computers and transporting equipment around
- I will keep my usernames and passwords secure
- I will not install any software or hardware (including memory sticks) without permission from a teacher
- I understand that if I am acting inappropriately, then my parents may be informed
- I will not take pictures of other children or adults without their permission.
- I will not send inappropriate pictures of someone to others when searching the internet
- I will choose the words that I put into the search engine carefully to eliminate the chance of inappropriate information being accessed.

Signed (Pupil) _____ Class _____

Date _____

Appendix C

Acceptable Usage Policy EYFS/KS1 Children – Linked to 360Safe AUP Guidelines

These rules have been written to make sure that you stay safe when using the computers. This includes cameras, netbooks, iPads and microphones too. By using the ICT in school,
you have agreed to follow these rules. Your teacher will talk about these rules before you sign them and a copy will be sent home to your parents.

If you have any questions, please ask your teacher.

The Golden Rule: **Think before you click**

☺ I will be careful when going on the Internet.

☺ I will tell a teacher if I see something that upsets me.

☺ I know people online might not be who they say they are.

☺ I will be polite when talking to people or writing online.

☺ I will think before I print or delete.

☺ I will be careful when using or carrying equipment.

☺ I will keep my password secret, but I can tell my family.

☺ Remember to log off properly.

☹ I won't tell anyone any personal details like my phone number or last name.

☹ I won't log on using someone else's username.

☹ Never put water bottles on the table when using ICT.

Signed (Pupil) _____ Class _____

Date _____