Working together to inspire every pupil to:
Step in to their learning adventure.
Step up to achieve their potential.
Step out and let their creativity shine.
Step together in friendship and respect.
Step forward and follow their dreams.

Address: Parkway, Chellaston, Derby DE73 5NY
Tel: 01332 691351
Web: www.homefields.derby.sch.uk

ICT and Email Acceptable Use Policy

Name of school: Homefields Primary School

Date of policy publication: September 2019

Author/s of policy: Homefields Primary School

Date of last review: September 2016 **Date of next review:** September 2022

Policy review dates and changes

Review date	By whom	Summary of changes made	Approved by
September 2019	M. Draper		Name: S.Coleman

Computing Coordinator – Milly Draper

ICT and Email Acceptable Use Policy Homefields Primary School

Basis for Policy

This Acceptable Use Policy is intended to provide a framework for the use of Homefields Primary School IT resources. It applies to all computing, telecommunication, and networking facilities.

IT systems are becoming increasingly critical for the day-to-day functions of governance, management, administration, parental links and involvement, teaching and learning. Computerised information technology resources available for governors, staff, parents and pupils will continue to grow and develop.

The protection of these resources is therefore of vital importance.

It is of equal importance that the community of users are themselves protected as far as is reasonably practicable from any potential harm that may result from unacceptable, uninformed and inappropriate use.

In order to facilitate the above every member of staff has to:

a) Understand what is and is not acceptable action and behaviour (acceptable use).
b) All users must take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally.
c) Agree to abide by and follow 'acceptable use' through the signing of an agreement.
d) Understand and accept that sanctions may apply for breaches of acceptable use and that this could include suspension, dismissal, exclusion or criminal prosecution.

Acceptable use is considered to be:

IT Equipment (including cabling)

1. Treat all equipment with care and respect so as to cause it no damage whatsoever.
2. Do not use any equipment that you believe to be damaged or unsafe.
3. Report immediately any damage to the equipment that you become aware of to the Network Manager.
4. Do not dismantle any part of the equipment.
5. Do not move any fixed equipment.
6. Do not relocate any piece of fixed equipment within the school unless you are authorised to do so.
7. Do not remove any part of the equipment from site unless you are authorised to do so. Bookable equipment is available in the Reprographics department.
8. If you are aware of anyone damaging, stealing or misusing equipment you must report it to a teacher or senior member of staff immediately.
9. Staff should not connect any equipment or device to the network without the prior approval of the Network Manager.

ICT and Email Acceptable Use Policy Homefields Primary School

Software

No person shall jeopardise the integrity, performance or reliability of computer equipment, software, data and other stored information. The integrity of the computer systems is put at risk if users do not take adequate precautions against malicious software.

1. Staff must not install, or attempt to install, programs of any type on a machine, or store programs on the computers without permission. The school will provide staff with specialist software to allow the user to trial software before installation on the network. This will help protect the laptop and the schools network from any form of malicious attack should the software be infected.
2. Staff must not deliberately damage, disable or otherwise harm the operation of software on computers.
3. Staff must not deliberately create, distribute or install agents designed to or are likely to hamper, disable, disrupt or damage any part of the IT infrastructure, equipment or software e.g. viruses, worms or bombs etc.
4. The distribution or storage by any means of pirated software is prohibited. Staff will be given a storage quota which will be set at 2.5GB. This will account for personal music, videos and photos in their work area, additional storage is available by request to the Network Manager, however needs to be justified.

Mobile Devices

1. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following classifications;
   • Laptop/notebook/netbook/tablet computers
   • Memory Sticks/USB Storage Media
   • PDAs
   • Any mobile device (including phones) capable of storing data
2. It is imperative that any mobile device be utilized appropriately and responsibly. The use of private equipment during lessons is forbidden unless there is a positive educational value.
3. Mobile phones must not be used during lesson time unless in an emergency.
4. It is the user's responsibility to ensure that no virus' are enabled through negligence. Any mobile device brought onto school premises should be virus free and checked on a regular basis.
5. It is the responsibility of any user who uses a mobile device to ensure the security of stored data. Data must not be downloaded and copied from the network or attached machines unless you have lawful and appropriate authority to do so.
6. All mobile devices should be password protected, and all data stored on the device should be encrypted using strong encryption. This password protection will be forced through the schools network policy to the mobile devices to ensure password protection is used.
7. The school reserves the right to refuse the ability to connect mobile devices to the school network infrastructure, if it feels such equipment is being used in a way that puts the school systems and data at risk.
8. The school accepts no responsibility for the safety of any such equipment and it is brought into school at the user's own risk.
9. Mobile devices belonging to the school must not be left unattended, i.e. in cars, or used by anyone other than staff members
10. Information about and photographs of staff/ pupils must not be taken or stored on any personal devices.

ICT and Email Acceptable Use Policy Homefields Primary School

Passwords and Security

All individually allocated usernames, passwords and e-mail addresses are for the exclusive use of the individual to whom they are allocated.

The user is personally responsible and accountable for all activities carried out under their username.

1. Staff must not disclose their password to others, or use passwords intended for the use of others. The password associated with a particular personal username must not be divulged to any other person, other than to designated members of IT staff for the purposes of system support.
2. Passwords used must adhere to current password policy and practice and should be changed immediately from any default password supplied.
3. Under no circumstances should any user disguise, attempt to disguise or mask their identity.
4. All users are expected to respect and not attempt to bypass security in place on the computer systems.
5. Attempts to access or use any username, e-mail address, which is not authorised to the user, are prohibited.
6. Users must not attempt to alter the settings of computers unless they are authorised to do so.
7. All users have a duty to respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.
8. All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
9. When leaving a computer unattended, you must ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence.
10. You should not store any sensitive or personal information about staff or students on any other portable storage system (such as a non-secure USB memory stick, portable hard drive, or laptop computer).
11. You must create a backup of any data which is not in relation to school on another storage system other than the school network. This includes any data on the local drive of your school provided laptop.

Commercial, Business, Buying and Selling

1. All work produced using school equipment/software resources are the property of the school. All work should not be erased from the system when an employee leaves the school.
2. Staff must not use the network/equipment/software for personal business interests unrelated to school business without prior approval.

Internet Rules

1. Staff must utilise access the Internet responsibly.
2. Staff must not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene, pornographic, abusive and are of an Adult Nature.
3. Staff must report accidental accessing of unsuitable sites to the Network Manager. The network manager will then liaise with the appropriate line manager to inform them.
4. Members of staff are expected to respect the work and ownership rights of people outside the school as well as other students and staff. This includes abiding by copyright laws; downloading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid licence, or other valid permission from the copyright holder.

5. The copying of other people's web site material without the express permission of the copyright holder is prohibited.

Use of social networking websites and online forums

Staff must take care when using social networking websites such as Facebook, Twitter or Instagram, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse;

- You must not allow any pupil to access personal information you post on a social networking site even for school-related purposes.
- You must not contact any pupil privately via a social networking website. You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, you must not post content on websites that may appear as if you are speaking for the school.
- You should not post any material online that can be clearly linked to the school that may damage the school's reputation.
- You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.

Privacy

The school has legal duties in respect of the safeguarding and protection of pupils. Staff are required by school policy to divulge the contents of any communication that they become aware of, to the Head Teacher or other nominated Child Protection Officer, if, in their opinion, the content gives rise to any potential concern for a pupils wellbeing. These communications may in turn be shared with other statutory bodies charged with child protection as required by law.

After a member of staff leaves, any data associated with the account will be considered to be the property of the school and the account will be closed. Data will be archived for a period in accordance with normal backup procedures prior to being deleted from the records held.

Legal

Any software and / or hard copy of data or information which is not generated by the user personally and which may become available through the use of school systems shall not be copied or used without permission of the school or the copyright owner. Such permission must be obtained in writing and in the event of the copyright owner not being the school; the school must be supplied with a copy of any permission obtained. It is up to the user to check the terms and conditions of any licence for the use of the software or information and to abide by them.

In the case of private work and other personal use of computing facilities, the school will not accept any liability for loss, damage, injury or expense that may result.

ICT and Email Acceptable Use Policy Homefields Primary School

Additional Information

Sections of note in association with this Acceptable Use Policy are;

- Data Protection Policy

Any suspected breach of this Acceptable Use Policy should be reported to the Network Manager or Business Manager. The responsible senior member will then take the appropriate action. IT staff will also take action when infringements are detected. The school reserves the right to audit and / or suspend without notice any account pending any enquiry.

This policy is not exhaustive and inevitably new social and technical developments will lead to further uses, which are not fully covered.

Staff should address questions concerning what is acceptable to either the Network Manager or Business Manager.

ICT and Email Acceptable Use Policy Homefields Primary School

E-Mail

Introduction

Homefields Primary School reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

Email is an educational and school business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Every employee has a responsibility to maintain the schools image and reputation. They also need to be knowledgeable about the inherent risks associated with email usage and to avoid placing the school at such risk. Although by its nature email seems to be less formal than other written communication, the same laws and business record requirements apply.

Awareness

It is important that users use the same level of care for other forms of the schools communication system and are aware of the legal risks of email usage to the school and individual. If you violate any of the policies within this policy, or violate any applicable laws, such as copyright infringement, you and Homefields Primary School can be held liable for damages and consequences.

By following this policy, the email user can minimize the legal risks involved in the use of email. If any user disregards the rules set out in this Email Policy, the user will be fully liable and Homefields Primary School will disassociate itself from the user as far as legally possible.

General Policies

The following rules are required by law and are to be strictly adhered to. It is prohibited to:

- Send objectionable material such as pornography and sexually explicit jokes.
- Use Homefields Primary School's email systems to engage in illegal, immoral, or unethical conduct
- Send discriminatory messages based on race, age, disabilities, gender, sexual orientation, or religious or political beliefs or other basis that is protected under applicable law
- Use email to advertise or otherwise support unapproved or illegal activities.
- Use email in any way that reflects poorly on Homefields Primary School's name, reputation and image.
- Exchange gossip about themselves or others, or rumors, exaggerated claims and unsubstantiated opinions relating to the school or individual employees.
- Send or forward emails with personal data, as these emails may become publicly accessible under Data Protection or Freedom of Information legislation
- Respond to any email that asks for personal or corporate account information, passwords or similar information. It is likely to be a phishing attempt. Immediately delete it.
- Send or forward emails with an attachment that contains a virus.
- E-Mail Contracts. Offers or contracts transmitted via e-mail are as legally binding on the school as those sent on paper.

ICT and Email Acceptable Use Policy Homefields Primary School

Can-Spam Act Policies

- Do not send or forward emails containing libelous, defamatory, offensive, harassing, hateful, racist, obscene or profane language or images. If you receive an email of this nature, you must promptly notify your Line Manager.
- Do not send unsolicited email messages.
- Do not forge or attempt to forge email messages.
- Do not disguise or attempt to disguise your identity when sending mail.
- Do not send email messages using another person's email account.
- Do not copy a message or attachment belonging to another user without permission of the originator.

Classified and Confidential

- It is prohibited to provide lists or information about Homefields Primary School employees to others and / or to send classified information without approval.
- Do not send or forward emails with corporate confidential, proprietary, sensitive, secure or trade secret information unless authorized by your supervisor to do so. Additional precautions should be taken when sending documents of a confidential nature. Employees who must transfer confidential documents via email are to ensure that the intended recipient is fully aware that the correspondence is 'CONFIDENTIAL'.
- Avoid using file names that might disclose confidential information. Confidential files should be password protected or encrypted. File protection passwords are to NOT be communicated via email correspondence in any event, and other arrangements are to be made for the disclosure of the password.
- Do not send or forward emails with comments, tips, or statements about company performance, sales, customers, orders, marketing efforts, plans or other confidential information that may negatively impact Homefields Primary School.
- Users must ensure that critical information is not stored solely within the e-mail system. Hard copies must be kept or copies stored separately on the system.
- Users are required to be familiar with the requirements of the Data Protection Act 1998 and to ensure that they operate in accordance with the requirements of the Act.

Personal Use

- It is strictly forbidden to use Homefields Primary School email system for anything other than legitimate educational and school business purposes. Therefore, the sending of personal emails, chain letters, junk mail, jokes and executables is prohibited.
- All messages and files distributed via the company owned email system, servers and transport mechanisms are Homefields Primary School's property and there should be no expectation of any privacy in any such messages or files.
- It is prohibited to conduct job searches, post information to bulletin boards, web logs (blogs), chat groups, list serves and the like without prior written approval from appropriate company management.
- It is prohibited to use company email for personal gain or profit
- It is prohibited to use personal email excessively or when it interferes with job responsibilities. This includes spending unreasonable and unwarranted time on Email activities.

ICT and Email Acceptable Use Policy Homefields Primary School

Passwords and Encryption

- All passwords must be made known to the company upon demand. The use of passwords to gain access to the computer or email system or to secure specific files does not provide users with an expectation of privacy in the respective system or document.
- Passwords should not be given to other people and should be changed once a month.
- Users may not encrypt any emails without obtaining written permission from their supervisor. If approved, the encryption key(s) must be made known to the company.

Email Retention

- All email header information, content and attachments are copied and archived into a separate location from the email server for an indefinite period of time and can only be deleted by authorized personnel according to the company retention policy schedule.
- Even after messages have been deleted from your account, and even from Homefields Primary School‘s archive system, they may still be stored on other company’s systems permanently and can most likely be recovered and presented at legal proceedings.

Email Accounts

- All email accounts maintained on our email systems are property of Homefields Primary School.
- No personal accounts shall be used for educational and school related business.

System Monitoring

- Users expressly waive any right of privacy in anything they create, store, send or receive on the company’s computer or network systems. Homefields Primary School will monitor, retrieve and reviewing email and file content without prior notification. If there is evidence that you are not adhering to the guidelines set out in this policy, the Homefields Primary School reserves the right to take disciplinary action, including termination and/or legal action.
- Homefields Primary School will use "surveillance software" to log, analyze and document use of email and supervisors may receive reports generated by such software. This may also be applied to transmissions from remote locations and from portable devices.

Receiving Unacceptable Email

- If you receive any offensive, unpleasant, harassing or intimidating messages via the Email you are requested to inform the head teacher or the ICT Support Department immediately. It is important that we trace such Emails as quickly as possible.
- Employees who feel that they have cause for complaint as a result of e-mail communications should raise the matter with the head teacher. If necessary the complaint can be dealt with under the grievance procedure.

ICT and Email Acceptable Use Policy Homefields Primary School

Usage Guidelines and Etiquette

Homefields Primary School considers email as an important means of communication and recognises the importance of proper email content and quick replies in conveying a professional image and delivering good customer service. Users should take the same care in drafting an email as they would for any other communication. Therefore Homefields Primary School advises users to adhere to the following guidelines:

- Writing emails:
    - All email messages must be appropriate and professional. Write well-structured emails and use short, descriptive subjects and clear sentences that are to the point. You may start your email with 'Hi', or 'Dear', and the name of the person.
    - The use of Internet abbreviations (Talk 2 U soon) and emoticons (☺) however, is not recommended.
    - Never use indecent, obscene, sexist, racist or other inappropriate language whether in written, cartoon, photographic or audio form.
    - Users must spell check all mails prior to transmission.
    - Do not write emails in all capitals as this may be interpreted as shouting, and is generally considered unprofessional.
    - Do not use cc: or bcc: fields unnecessarily or excessively.
    - Ensure that everyone copied knows what action, if any, to take.
- Attachments:
    - Do not send unnecessary attachments.
    - Compress attachments larger than 2Mb before sending them, if possible.
    - Great care should also be taken when attaching documents as the ease with which employees can download files from the Internet or cut and paste, materials from electronic sources increases the risks of infringement of the rights of others particularly the intellectual property and other proprietary rights. Also attaching documents may give rise to the release of information not intended to be disclosed.
- Maintenance:
    - Folders that should be deleted on a regular basis include "Deleted Items", "Junk Mail" and "Sent Items" folders.

Questions

If you have any questions or comments about this Email Policy, please get in contact with the Network Manager or the Business Manager. If you do not have any questions Homefields Primary School presumes that you understand and are aware of the rules and guidelines in this Email Policy and will adhere to them.

ICT and Email Acceptable Use Policy Homefields Primary School

Declaration

I have read, understand and acknowledge receipt of the ICT and Email Acceptable Use Policy. I agree to be bound by and will comply with these polices and guidelines. I understand that any violation of these Policies may subject me to disciplinary action, up to and including dismissal, as well as possible civil and criminal penalties.

Signature: _____ Date: _____

Printed Name: _____