# Gaskell Community

# Primary School

# Acceptable Use Policy

**September 2021**

## Version Control

| Current version | Previous version | Summary of changes made |
|---|---|---|
| 18 | 01 Sep 13 | Change of policy title from Email, Internet Security and Facsimile Policy. Sections and appendices renumbered. Formatting of paragraphs, headings and appendices standardised. |
| | | |
| | | |
| | | |

## Contents

# 1 Introduction

1.1 The increasing use of Information and Communications Technology necessitates a security policy to ensure these systems are developed, operated and maintained in a safe and secure manner.

1.2 The internet is the single most significant and unique development in information technology in recent years. It has evolved into a worldwide open environment of networked PCs and computer services, whose whole purpose is to facilitate the open exchange of information.

1.3 The internet can be utilised to provide significant business benefits, particularly in respect of promoting the school's image to the outside world. However, it's very openness makes it vulnerable to security threats, and appropriate controls are required to minimise these risks.

1.4 The policy will apply to all staff who need to be aware of the importance of information security and their responsibilities for security whilst working in school premises or off site.

1.5 It is not the intention of the policy (or resultant security controls) to be unnecessarily restrictive. The aim of the policy is to ensure there is a framework of control in place for mitigating significant risks to the school's information services, its employees and its image.

1.6 The policy is binding on all employees who are authorised to use email, the internet or the facsimile systems for school business and must be adhered to at all times.

# 2 Guiding principles

2.1 The policy has been drawn up having regard to the following guiding principles:

- To outline the strategic framework and responsibilities for maintaining effective security over the school's internet, email and facsimile systems.
- To ensure appropriate levels of:

    i. **Confidentiality** - ensuring information is not disclosed inappropriately.
    ii. **Integrity** - safeguarding the validity, accuracy and completeness of information owned, obtained and used by the school.
    iii. **Availability** - ensuring that information is accessible and usable when required for the business of the school.
    iv. **Relevance** - ensuring that the internet, email and facsimile systems are used in accordance with the business needs of the school.

2.2 The policy has been drawn up in accordance with current statutory provisions relating to information systems including;

- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Data Protection Act 2018
- Computer Misuse Act 1990

- Copyright, Designs and Patents Act 1988
- Obscene Publications Act 1964
- Equality Act 2010

# 3 Appropriate use of information systems

3.1 Communication resources belong to the school and are to be used solely for school business. However, where an employee has access to the equipment out of business hours or has obtained appropriate permission to use the equipment, and where there is no extra cost to the school, employees are encouraged to develop their skills, knowledge and understanding of the email and internet as long as these systems are used reasonably and appropriately.

3.2 As a general principle, internet access, email and facsimile facilities are provided to employees to support them in their work related activities. The following list, although not intended to be definitive, sets out broad areas of use that the school considers to be appropriate:

- to provide a means of business communication within the school and other schools, agencies and organizations
- to view and obtain information in direct support of the school's business activities
- to promote services and products provided by the school
- to communicate and obtain information in support of approved personal training and development activities
- any other use that directly supports work related functions

3.3 It is each employee's responsibility to check with their Head Teacher to ascertain whether any proposed use, not referred to in the above paragraph, falls within the school's definition of appropriate use.

3.4 The use of the school's systems to communicate Trade Union business is laid down in the school's Facilities Agreement.

3.5 Any abuse or misuse of the school's communication resources by an employee may be considered a disciplinary offence.

3.6 Some examples of what could constitute a disciplinary offence under the policy are:

- contravention of a legal provision, e.g. Regulation of Investigatory Powers Act 2000, Freedom of Information Act 2000, Data Protection Act 2018, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988, Obscene Publications Act 1964, Equality Act 2010; or any internal school policy (in particular Equality Policy) is unacceptable; see also Social Networking Policy
- use of equipment without prior consent
- circulation of personal information, for example advertisements, offers to sell goods
- introduction of viruses
- viewing, downloading or circulating illegal or offensive material from the internet
- unauthorised viewing of other people's emails
- use of email for potential offensive or defamatory purposes

- hacking into other people's emails and systems
- unauthorised alteration of data
- circulation of malicious, racist, sexist or offensive material including chain letters

3.7 Employees should be aware that any of the above could also constitute a criminal offence.

# 4 Equipment security

## Security of equipment off premises

4.1 The use of equipment off-site must be formally approved by your line manager. Equipment taken away from school premises is the responsibility of the user and must;

- be logged in and out
- not be left unattended
- concealed whilst transporting
- not left open to theft or damage whether in the office, during transit or at home
- where possible, be disguised (e.g. laptops should be carried in less formal bags)
- be encrypted if carrying personal or confidential information
- be password protected
- be adequately insured (please contact the insurance section for further details)

# 5 Copyright and licensing

5.1 All employees are responsible for ensuring that copyright and licensing laws are not breached. If in doubt you can seek advice from Local Authority Legal Services.

# 6 Email acceptable use policy

6.1 This section states how you should make use of the email facility that the school has provided for your work. It outlines your personal responsibilities and tells you what you must not do. All email prepared and sent from school email addresses or mailboxes, and any non-work email sent using school ICT facilities is subject to this policy.

6.2 The email system is provided to allow electronic communication in pursuance of school business between school employees and external organisations.

6.3 The emails that you produce (work or non-work related), send and receive are the property of the school. It is important to remember that an email forms part of the administrative records of the school and managers have the right of access to all emails, sent or received, on the same basis as any other written documentation.

6.4 Line Managers may request access to emails where staff are absent for long periods or information needs to be accessed urgently. Managers must inform employees in this situation.

6.5 Managers should only request access to work related information, where there is a legitimate business need. School's ICT may request approval from a more senior

manager. Misuse of this access will be considered seriously under the appropriate policy at the time.

6.6 The school will provide a secure environment to host your email facility. This security framework includes a login details and password facility.

6.7 You are responsible for the security provided by your login details. You should not disclose your login details or password to anyone. Emails sent from your account are deemed to have been sent by you.

6.8 You may only use the email accounts that you are authorised to access.

6.9 Email communications held by or on behalf of the school may be subject to the Freedom of Information Act 2000, so that anyone may be entitled to access to them, unless exempt from disclosure under the Act. Therefore you must be aware that the school may be required to disclose your emails or responses to them under the Act.

6.10 In order to ensure compliance with the requirements of the school and the contents of this policy, monitoring software will be utilised to check on the use of email, as well as software to check the content of email messages sent and received.

6.11 These software tools will only be used for the legitimate purposes of ensuring compliance with stated legal acts, policies and guidelines so as to protect the school against the risk of criminal and civil actions, as a result of the unauthorised actions of its employees, and in connection with the administration of the email system itself.

6.12 Employees should be aware that email messages could ultimately be required to be disclosed in Court.

6.13 Be aware that the school will regularly monitor your email account usage and email content. The school reserves the right to monitor email communications and records without notice.

## Emails as records

6.14 By its nature, email seems to be less formal than other written communications, however it must be noted that email is a written record and the same laws apply. Both the school and the individual can be held liable for any illegal use of the email system, including sending or forwarding libellous, breach of trust, defamatory, offensive, harassing, racist, obscene or pornographic remarks or depictions (for further details see Do and Don't section).

6.15 It should also be noted that agreements or contracts entered into via email are as binding as a written document. Therefore it is the responsibility of each employee to ensure that the content of emails are correct, whether they are sending or receiving emails.

6.16 Non-school email accounts must not be used to conduct or support official school business.

6.17 The information below contains the email do's and do not's you need to be aware of. Do;

- be aware that email systems will be monitored when it is necessary and appropriate
- respect the confidentiality of the school and of those who send you information
- contain appropriate contact details including Full name, address and telephone number
- include an appropriate Subject line for the email
- respect password privacy and be vigilant of 'hackers'
- file and store information correctly and safely
- take advantage of the appropriate training
- discuss with your Manager any issues you may have, and if necessary ask for a copy of the Policy
- ensure appropriate use of language as email messages can be misconstrued
- Be aware if sending sensitive data in email within the school network that, with mobile access, emails may be viewed in public places

6.18 Do not;

- infringe copyright and licensing laws
- distribute material containing offensive language, offensive images or chain letters
- distribute inappropriate emails e.g. unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, internally or to other organisations
- spread gossip, rumours, and innuendos about employees, clients, partners or 3rd parties
- forward virus warning on to other users unless authorised
- distribute material that is intended to alarm others, embarrass the school, negatively impact on employee productivity or harm employee moral
- send full videos or clips, photographic or cartoon images, jokes or 'joke' chains
- send entertainment software, other non-work related software, games or gambling by email
- play games with opponents over the email system
- register your email address on websites that do not relate to school business
- hack into emails you are not authorised to access
- forward school emails or attachments from your school email address to your home (private) email address
- attempt forgery of emails
- introduce viruses or other malware/spyware
- store obsolete and out of date information (unless still useful for business purposes)
- use the school's resources without permission

6.19 The above list gives examples of "Unsuitable" material but is neither exclusive nor exhaustive.

6.20 If an employee receives an email that is considered to be offensive or malicious then they must consult their line manager. In such circumstances these emails should not be responded to.

## Personal use of the school's email system

6.21 Provided it does not interfere with your work, the school also permits 'occasional and short' use of the email system for personal communications. 'Occasional and short' means infrequently and for seconds, rather than minutes. You are not allowed to use the system for personal 'conversational' email.

6.22 Any personal or private emails sent must be marked as such in the Subject field. If you are in any doubt about how you may make personal use of the system, then you are advised not to use it for personal use.

# 7 Internet acceptable use policy

7.1 This section tells you how you should use your school internet facility. It outlines your personal responsibilities and tells you what you must and must not do.

7.2 The school recognises that it is not practical to define precise rules that cover the full range of internet activities available and in general, it is adherence to the spirit and essence of the policy that will allow the school as a whole, and employees in person, to productively benefit from access to this powerful technology.

7.3 The internet facility is made available for the business purposes of the school. A certain amount of personal use is permitted in accordance with the statements contained within this policy.

7.4 The internet service is primarily provided to give school employees;

- access to information that is pertinent to fulfilling the school's business obligations
- the capability to post updates to school owned or maintained websites
- access to research
- access to, and provision of, information
- an electronic commerce facility (e.g. purchasing equipment for the school)

## Personal use of the school's internet facility

7.5 At the discretion of your line manager, and provided it does not interfere with your work, the school permits personal use of the internet in your own time (for example during your lunch-break).

7.6 If you are in any doubt about how you may make personal use of the system, then you are advised not to use it for personal use.

7.7 All personal usage must be in accordance with this policy. Your computer and any data held on it are the property of the school and may be accessed at any time by the school to ensure compliance with all its statutory, regulatory and internal policy requirements.

## Internet account management, security and monitoring

7.8 The school will provide secure login details and password facility for your internet account. You are responsible for the security provided by your login details and

password. You should not disclose your login details and password to anyone. Any internet activity from your account is deemed to have been carried out by you.

7.9 The provision of internet access is owned by the school and all access is recorded, logged and interrogated for the purposes of;

- monitoring total usage to ensure business use is not impacted by lack of capacity
- the filtering system monitors and records all access for reports that are produced for line managers and auditors
- ensuring compliance with this policy, legal acts, policies and guidelines
- protecting the school against the risk of criminal and civil actions

7.10 Various categories of websites are currently blocked using a URL filtering system, for example;

- adult material (excluding sex education)
- MP3, audio download services and streaming media
- games, gambling, internet auctions
- illegal or questionable
- hacking, proxy avoidance and peer-to-peer
- web email, chat, instant messaging and text messaging
- militancy and extremist
- racism and hate, tasteless
- personals, dating, social networking and personal sites
- violence, weapons and illegal drugs

7.11 Although the school uses filtering software to automatically block access to websites, appropriate use of the internet facility still remains your responsibility.

7.12 Except where it is strictly and necessarily required for your work, for example IT audit activity or other investigation, you must not use your internet account to;

- Create, download, upload, display or access knowingly, sites that contain pornography or other ‘unsuitable’ material that might be deemed illegal, obscene or offensive. Unsuitable material would include data or images the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of this and other school policies
- Spread gossip, rumours, and innuendos about employees, clients, partners or 3rd parties on blogs, newsgroups, forums or Social Networking sites.
- Spread derogatory or inappropriate comments about your employment colleagues, employees or its partner organisation on blogs, newsgroups, forums or Social Networking sites.
- Write or present views on behalf of the school on blogs, newsgroups, forums or Social Networking sites, unless authorised by the school.
- Display photographs on Social Networking sites, that portray you in a way that could bring the school into disrepute.
- Include children or young people that you are associated with through your work into your friends or contacts lists.
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.

- Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs.
- Subscribe to, enter or use online gaming or betting sites.
- Subscribe to or enter ‘money making’ sites or enter or use ‘money making’ programs.
- Run a private business.

7.13 The above list gives examples of unsuitable usage but is neither exclusive nor exhaustive.

7.14 Do;

- be aware that telecommunication systems will be monitored when it is necessary and appropriate
- conduct yourself in an honest and professional manner
- be aware of the addictive qualities of the internet
- take advantage of the appropriate training
- discuss with your Manager any issues you may have, and if necessary ask for a copy of the policy

7.15 Managers should seek to ensure that the internet facility is used appropriately and in direct relation to the work of an employee. Managers should make employees aware of the potential addictive qualities of the internet and the use of computers in general.

# 8 Etiquette and user responsibilities

8.1 Employees need to be mindful that they are acting as representatives of the school when using school equipment.

8.2 Whilst employees can expect the school to respect their privacy there are certain exceptions, in relation to the communication systems where staff should be aware that there is routine monitoring by the school outlined in Section 9.

8.3 Although each employee has a password to their computer, this does not guarantee private viewing. Hackers can enter networks; information transmitted can also be captured by other websites.

8.4 Head Teachers should seek to ensure that the internet and email is used appropriately and in direct relation to the work of an employee. Head Teachers should make employees aware of the potential addictive qualities of the internet and the use of computers in general.

8.5 Head Teachers should ensure, through the Personal Development Plan process that appropriate training is made available to employees who have access to school’s information and communication systems.

8.6 Head Teachers are responsible for ensuring employees understand their rights and responsibilities with regard to the use of the school’s communication systems. Head Teachers must ensure employees receive a copy of this policy and any subsequent amendments, along with a copy of the Employee Declaration at Appendix B.

8.7 Employees should be aware that leaving their password by their terminal or leaving their terminal on overnight renders security systems ineffective. Employees should therefore ensure that terminals are switched off at the end of the working day and passwords are kept secure.

8.8 Employees who have access to laptops, and any other mobile equipment, are r Employees should be familiar with the contents of this Policy.

8.9 Responsible for the safety and security of any such equipment.

8.10 Employees must ensure they do not deactivate the virus scanners on their systems.

8.11 If an employee unintentionally accesses a website which contains material of an offensive or undesirable nature, they should immediately exit the site. In such a situation an employee should report the incident to the Head Teacher who may prevent future access to such sites by implementing preventative measures having consulted with Schools' ICT. Websites relating to sex, gambling etc. are routinely recorded and reported to Head Teachers as applicable.

# 9 Monitoring

9.1 The school, when monitoring, will ensure it complies at all times with the relevant legislation and guidance, including;

- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Data Protection Act 2018
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

9.2 The regulations allow business and public authorities to record or monitor communications without consent in such cases as;

- recording evidence of transactions
- ensuring compliance with regulatory or self-regulatory rules or guidance
- gaining routine access to business communications
- maintaining the effective operation of the systems
- monitoring standards of service and training, and
- combating crime and the unauthorised use of systems

9.3 The school reserves the right accordingly to monitor email communications and records without notice.

**APPENDIX A**

# ICT acceptable use do's and don'ts

Bolton Council

Worldwide the email and internet are increasingly used as a means of communication along with the use of faxes.

Whether you use these systems or not, you should be aware that we all represent the school and are accountable to the public.

Therefore to ensure the protection of the school, its employees and all other authorised users, the school's ICT Acceptable Use Policy has been produced. The policy makes it a disciplinary offence to abuse or misuse the School's communication and information systems.

The policy is binding on all employees and users of the systems. Access to the full document can be gained through the Head Teacher.

As an Employee you have a responsibility for the way you use the School's email, internet and telecommunication systems. The information below covers the main do's and don'ts you need to be aware of.

## Do

- Be aware that telecommunication systems will be monitored when it is necessary and appropriate
- Respect the confidentiality of the School and of those who send you information
- Respect password privacy and be vigilant of 'hackers'
- File and store information correctly and safely
- Be aware of the addictive qualities of the 'Net'
- Take advantage of the appropriate training
- Discuss with your Head Teacher any issues you may have, and if necessary ask for a copy of the Policy
- Ensure lap tops and any other mobile equipment is kept secure at all times
- Ensure appropriate use of language as email and fax messages can be misconstrued

## Do not

- Infringe copyright and licensing laws
- Distribute material containing offensive language, offensive images or chain letters
- 'Hack' into files you are not authorised to access
- Store obsolete and out of date information
- Access inappropriate websites
- Use the School's resources without permission

**APPENDIX B**

# Employee declaration

Bolton Council

| Employee details | |
|---|---|
| I confirm that I have received a copy of the school's ICT Acceptable Use Policy. I have read and understood the policy and am aware that should I contravene the requirements contained in the policy disciplinary action may be taken. | |
| **Name** | |
| **Job Title** | |
| **School** | |
| **Signed** | **Date** |

Please send your completed declaration to your Head Teacher.

| Authorisation | |
|---|---|
| To be completed by the Head Teacher. | |
| **Name** | |
| **Signed** | **Date** |