Acceptable Use Policy

Mission Statement:

'In St Margaret Mary's School
we welcome everyone into our community
in order to live, love and learn
together in the light and example of the life of Christ.'

Policy to be reviewed July 2022

St Margaret Marys Catholic Primary School

Acceptable Use Policy
Birmingham Education Service Policy for the Acceptable Use of the Internet

The policy set out below is that which has been agreed for the acceptable use of the Internet within Birmingham Education Department. All schools should also have an acceptable use policy both for pupils and staff. Guidelines on producing such a policy are given on our Policy Guidelines page.

All of the guidelines have been produced in the light of current legislation including the following Acts. Please click the name of each Act for the full wording.

- **Copyright, Designs and Patent Act (1988)**
- **Human Rights Act (1998)**
- **Regulation of Investigatory Powers Act (2000)**
- **Data Protection Act (1998)**

PART 1 - INTRODUCTION

1.1 Purpose

This is a corporate statement of good computer practices to protect the Department (Education Services) from casual or intentional abuse. With the growth in use of e-mail and access to the Internet throughout the organisation, there are a number of threats and legal risks to the Department, as well as the potential costs of time wasting, that can be avoided by following the practices outlined.

Although both these tools are provided first and foremost for business use, the City Council and the Department accept that on occasion they may be used for personal use. At all times users should take into account these guidelines and adhere to them.

1.2 Scope

These guidelines apply to all employees who have access to e-mail or the Internet.

1.3 Publicising the guidelines

Effective communication is vital to increase staff awareness of these guidelines and their use within the Department. All users will be notified of the Acceptable Use Policies for E-mail and the Internet to which these guidelines refer, via a logon screen which will appear whenever a user logs-on. To proceed, users will have to click on a button that states "By clicking here I accept all City Council and Education Services policies on the use of computers including e-mail and the Internet".
In addition, all such policies and guidelines will be available on-line.
Further, new starters should not be given access to e-mail or the Internet until they have seen and accepted these policies. This will be the responsibility of their line manager in respect to the Induction checklist issued on the new starter's arrival.

Any major revisions to these policies or guidelines will be notified via e-mail.

1.4 Monitoring

The Department and the City Council has 3rd party "firewall" software and systems in place to monitor all Internet usage and these will be checked and analysed on a regular basis. Certain sites will be blocked if they are deemed to hold inappropriate or sexually explicit material.

Although the Department respects the privacy of every individual throughout the organisation, all external mail (both incoming and outgoing) will be checked for content and attachments to make sure that at all times the security and integrity of the Department is not impeded. The sender of any message that is intercepted will be notified immediately.

1.5 Disciplinary Process

Action will be taken under the City Council's Disciplinary Policy against any users who are found to breach the policies outlined in these guidelines.
Significant abuse, particularly involving access to pornographic or offensive or images constitute gross misconduct leading to summary dismissal.

PART 2 - RESPONSIBILITIES

2.1 DMT

The policies and these guidelines have been approved and adopted by the Department Management Team.

2.2 Managers & Supervisors

It is the responsibility of all managers and supervisors that the policies and guidelines are properly implemented and policed.

2.3 Learning and Culture IT

Learning and Culture IT will ensure that users are notified of their responsibilities with regard to the use of e-mail and the Internet. Through the use of 3rd party "firewall" software, Learning and Culture IT will monitor Internet and e-mail use and the subsequent analysis of this data (in accordance with the Internet and E-mail Analysis procedure). Also, the appropriate security virus prevention mechanisms will be maintained and updated to meet the ongoing requirement of the Department (in accordance with the Virus Protection procedure).

2.4 Employees

All staff, with access to e-mail and the Internet, will be held responsible for complying fully with the Department's computer policies and guidelines.

PART 3 - E-MAIL GUIDELINES

3.1 Personal Use

Employees are permitted to send personal e-mails on a limited basis (in accordance with the City Council IT Security Policy - Computer Misuse) as long as this does not interfere with their job responsibilities. It should be noted that any e-mail messages are not guaranteed to be private and remain the property of Birmingham Education Services.

3.2 Confidentiality

Messages sent and received via the Internet are regarded by the Company's Act as having the same legal status as a corporate letter. Any material that is viewed as highly confidential or valuable to the Department should not be e-mailed externally.

A disclaimer document will be attached to all e-mails with an individual signature for each user. In no instance should the disclaimer be tampered with, although if necessary the signature can be altered.

It should be remembered that the Internet does not guarantee delivery or confidentiality.

It should be noted that there are systems in place that can monitor, review and record all e-mail usage, and these will be used. Analysis of this information may be issued to managers if thought appropriate. No user should have any expectation of privacy as to his or her e-mail.

3.3 Etiquette

At all times users should use appropriate etiquette when writing e-mails, e.g. emails should not be written in capitals as this can be perceived as 'shouting'. Guidance on "netiquette" is provided in the appropriate City Council and Education Services policies and guidelines. These include warnings about the need to be careful about addressing e-mails, particularly when using address groups, in order to send them to only those recipients who will have an interest.

In some instances, where the nature of a message may be deemed confidential, it may be appropriate to notify, or even seek permission from, the original sender before forwarding a message onto another recipient.

3.4 Dissemination of Information

In cases where information of a general nature is circulated via e-mail of on an electronic notice board, database or web site, it is the responsibility of the relevant manager or supervisor to ensure that members of their staff who do not have access to the system are notified of the information.

Please note that, even though there is no current case law, it is possible that e-mail could be covered by Data Protection legislation

In particular, we are advised that the legislation will apply (1) if e-mails identify individuals are filed or organised in a structured manner that could be constituted as a "file", and (2) to documents "attached" to e-mails if they identify individuals.

Also, under legislation, individuals have to give permission for data concerning them to be shared particularly if via the Internet.

So, care needs to be taken regarding e-mailing information that could be linked to a named individual: please consult the Data Protection Officer if in doubt. This also applies to information shared on the BGFL Teams platform.

3.5 Inappropriate behaviour

Users should not send messages that contain any unsuitable material or defamatory statements about other individuals or organisations.

Messages should not contain material or language that could be viewed as offensive to others or as contravening the City Council Equal Opportunities Policy, N.B. what may appear appropriate to one person might be misconstrued by another.

3.6 Canvassing, lobbying, advocacy or endorsement

Material, which could be construed as canvassing, lobbying, advocacy or endorsement should not be sent by e-mail, particularly if this is commercially- or politically- based, and more particularly if this it expresses a personal, rather than a City Council or Education Department, view.

If in doubt, consult your line manager.

3.7 Virus Protection

To prevent the risk of potential viruses, users should not open any unsolicited e-mail attachments or independently load any software, including screensavers, onto their computers. If a user does inadvertently open a message or attachment that contains a virus, they need to contact the Learning and Culture IT Help Desk immediately and close the message and attachment. It should not be accessed again without approval from Learning and Culture IT.

In some instances it might be appropriate to inform the original sender that their message contained a virus. Further details of the virus can be obtained from Learning and Culture IT.

3.8 Security

E-mail is an effective way of communicating confidential information. This is only the case, however, if passwords are secure. To maintain security it is good practice for users to change their passwords regularly (further information can be found in the City Council IT Security Policy).

E-mail should not be left running unattended in any circumstances where this may lead to unauthorised access. The system should be closed and re-opened on return. In no instances should a user login using a colleague's password unless permission has been given.

Where access to a mailbox is required, Learning and Culture IT can setup temporary passwords. Prior permission must be received from the individual concerned or their senior manager.

3.9 Housekeeping

Good housekeeping practices should be adopted so that files are deleted regularly or, if necessary, archived to a separate file. Mailbox sizes will be reviewed regularly and warnings will be issued to users with files of 50MB or larger. In future, it is likely that mailbox files will have a maximum size.
File attachments, incoming or outgoing through the firewall, are limited to 15MB but good practice is that file attachments should only be sent to a minimum of recipients and not all if they are large files. The guidance notes, particularly on the Management of E-mail, make this clear.

3.10 Email / Google Drive

When using Google Classroom and the Gsuite Apps, students will use approved class email accounts under supervision of a teacher or parent/guardian. Students will not send or receive any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person. Students will not reveal their own or other people’s personal details, such as addresses or telephone numbers or pictures. Students will never arrange a face-to-face meeting with someone they only know through emails or the Internet.

3.11 Online Chat

Discussion forums on Google Classroom will only be used for educational purposes and will always be supervised. Students will never arrange a face-to-face meeting with someone they only know through emails or the Internet and this is forbidden.

PART 4 - INTERNET GUIDELINES

4.1 Rules for business use

All users will be provided with access to the Internet through the Birmingham Grid for Learning but line managers should approve usage.

Users should not download any material that is not directly related to their job responsibility. This especially relates to screensavers, images, videos games etc. Learning and Culture IT should be notified before any software is downloaded for business use: all downloaded software needs to be properly licensed and registered. Any such software automatically becomes the property of the City Council. There are systems in place to monitor all Internet usage including any software downloads.

4.2 Personal use

Employees are permitted to access the Internet for personal use on a limited basis with the approval of their line management (in accordance with the City Council IT Security Policy - Computer Misuse) as long as this does not interfere with their job responsibilities. This should be in own time, i.e. when clocked-out, or with the permission of line management.

It should be noted that there are systems in place that can monitor and record all Internet usage, and these will be used. No user should have any expectation of privacy as to his or her Internet usage. Analysis of this information may be issued to managers if thought appropriate.

4.3 Respecting copyright

Employees with Internet access must comply with the copyright laws of all countries relevant to Education Services. Users must not intentionally download any material that holds a copyright notice. This also relates to downloading and copying unlicensed software.

4.4 Security

Systems are in place to protect the Department's information systems. However users must also be aware of the potential risks associated with accessing the Internet. Employees are reminded that newsgroups are public forums where it may be inappropriate to reveal confidential information.
Also, see section 4.2 above.

Users are also reminded that unauthorised usage of a computer could include accessing e-mail or the Internet via a computer other than your own even if doing so under your own user identification, and could contravene City Council ICT Security Policy and even Computer Misuse legislation.

4.5 Virus protection

Although virus protection software is installed on all networked computers, users should be aware of the potential hazards associated with computer viruses. Any files that are downloaded will be scanned for viruses before being accessed. If you have any concerns about viruses on the Internet or think you may have accessed material that contains a virus please contact the Education IT Help Desk.

4.6 Inappropriate websites

Under no circumstances should a user access a site that contains sexually explicit or offensive material. If you find yourself connected to such a site inadvertently, you should disconnect from that site immediately, and notify your line manager.

Because individuals may consider a wide variety of material offensive, users should not store, view, print or redistribute any material that is not directly related to the user's role or the Department's activities.

H.Coates
Computing Coordinator
To be reviewed July 2022