ST MATTHEW'S C OF E PRIMARY SCHOOL

Internet Usage Policy

Part 1 – Introduction

1.1 Purpose

This is a school statement of good computer practices. To protect the school from casual or intentional abuse of internet usage. With the growth in use of e-mail and access to the Internet throughout the school, there are a number of threats and risks to the school, as well as the potential costs of time wasting, that can be avoided by following the practices outlined.

The school accepts that on occasions the internet 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.

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

1.3 Publicising the guidelines

Effective communication is vital to increase staff awareness of these guidelines and their use within the school. All users will be notified of this policy.

New members of staff will not be given access to e-mail or the Internet until they have signed for and accepted the terms of this policy. This will be the responsibility of their line manager in respect of the induction of new members of staff.

Any major revisions to this policy will be notified via whole staff meetings.

1.4 Monitoring

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 school respects the privacy of every individual throughout the school, all external mail (both incoming and outgoing) may be checked periodically for content and attachments to make sure that at all times the security and integrity of the school is not impeded.

1.5 Disciplinary Process

Action may be taken under the schools Disciplinary Policy against any users who are found to breach this policy may constitute gross misconduct leading to summary dismissal.

Part 2 – E-mail Guidelines

2.1 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.

2.2 Confidentiality

Messages sent and received via the Internet are regarded by the school as having the same legal status as a school letter.

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

2.3 Dissemination of Information

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

Care needs to be taken regarding e-mailing information that could be linked to a named individual: please consult the Data Protection Policy if in doubt.

2.4 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.

2.5 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 the Headteacher.

2.6 Virus protection

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

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

2.7 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 set up temporary passwords. Prior permission must be received from the individual concerned or their senior manager.

2.8 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.

Part 3 – Internet Guidelines

3.1 Rules for business use

All users will be provided with access to the Internet through the Birmingham Grid for Learning.

Users should not download any material that is not directly related to their job responsibilities. This especially relates to screensavers, images, video 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.

3.2 Personal use

Employees are permitted to access the Internet for personal use 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. This should be in own time 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.

3.3 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.

3.4 Security

Users must be aware of the potential risks associated with accessing the Internet. Employees are reminded that newsgroup forums where it may be inappropriate to reveal confidential information. Also, see section 4.2 above.

Staff should be aware that regardless of the PC they are using the should not contravene City Council ICT Security Policy and even Computer Misuse legislation

3.5 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 Link2ICT Help Desk.

3.6 Inappropriate websites

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

Policy Author:	*Deborah Murdock*
Approved by/when:	*Governing Body Periodically*
Date of last approval:	*14th June 2017*
Due for review:	*June 2019*