

Beaufort and LANGLEY SCHOOLS

INTERNET SAFETY POLICY

Our Internet Policy has been written by the schools building on the Birmingham BGfL policy and government guidance. All users are required to agree to the acceptable use policies for e-mail and internet via the Policycentral login screen which states '*This computer network has an Acceptable Use Policy (AUP) related to all computer, related equipment, network and internet use. Any such use which is found to include inappropriate, suggestive, confidential or illegal material to the detriment of it's owners or other users and which has been transmitted, received or created on this computer is a violation of the AUP. Any individual found to be in violation of this AUP will be subject to disciplinary action. The computer, related equipment, network and internet is not for personal use. If you do not understand the information contained in this policy, please contact a member of management immediately.*'

This policy has been agreed by the senior management and approved by governors.

1 The importance of the Internet

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

2 Educational benefits of the Internet

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in government initiatives such as the DfE ICT in Schools and the Virtual Teacher Centre (VTC) <http://vtc.ngfl.gov.uk>;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LA and DfE

3 Enhanced Learning through Internet use

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

4 Evaluation of Internet content

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

5 Management of e-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others in e-mail communication, such as, address or telephone number, or arrange to meet anyone.
- Whole-class or group e-mail addresses should be used.

6 Management of Web site content

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

7 Newsgroups and e-mail lists

- Newsgroups and e-mail lists will not be made available to pupils unless an educational requirement for their use has been demonstrated.

8 Chat room safety

- Pupils will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.

- A risk assessment will be carried out before pupils are allowed to use a new technology

9 Management of emerging Internet applications

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

10 Authorisation of Internet access

- The school will keep a record of any pupils whose parents have specifically denied internet or e-mail access.
- Access to the Internet will be initially by adult demonstration followed by directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised Internet access (an example letter for primary schools is included as an appendix).
- Parents will be asked to sign and return a form stating that they have read and understood the Acceptable use document. Appendix A

11 Risk assessment

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor BCC can accept liability for the material accessed, or any consequences of Internet access.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher will ensure that the Internet Safety policy is implemented and compliance with the policy monitored.

12 Management of filtering

- The school will work in partnership with parents, the LA, Dfe and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to BCC using the e-mail filtering@bgfl.org via the E-Safety co-ordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Filtering strategies will be selected by the school, in discussion with BCC. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

13 Ensuring pupil awareness of Internet Policy

- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- Pupils will be reminded of the rules and risks at the beginning of any lesson using the Internet

14 Ensuring staff awareness of Internet Policy

- All staff are governed by the terms of this policy in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the Internet Safety Policy, and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in safe and responsible Internet use and on the Internet Safety policy will be provided as required.

15 Maintenance of the ICT security system

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.
- Files held on the school's network will be regularly checked.
- The IT co-ordinator / network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

16 Complaints procedures regarding Internet use

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

17 Parental Support and Awareness

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school Web site.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.

Reviewed February 2016

Appendix to Internet Safety policy

Use of ICT: All adults working in school

All users are required to agree to the acceptable use policies for e-mail and internet via the Policycentral login screen which states '*This computer network has an Acceptable Use Policy (AUP) related to all computer, related equipment, network and internet use. Any such use which is found to include inappropriate, suggestive, confidential or illegal material to the detriment of its owners or other users and which has been transmitted, received or created on this computer is a violation of the AUP. Any individual found to be in violation of this AUP will be subject to disciplinary action. The computer, related equipment, network and internet is not for personal use. If you do not understand the information contained in this policy, please contact a member of management immediately.*'

Monitoring of ICT

The School 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 School 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 School 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.

2.3 Link2ICT

Link2ICT 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, Link2ICT 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 School (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 School's computer policies and 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 School 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.

3.5 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.

3.7 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 Link2ICT Help Desk immediately and close the message and attachment. It should not be accessed again without approval from Link2ICT.

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 Link2ICT.

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. Link2ICT 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.

4.6 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 School's activities.

Reviewed February 2016