SLADEFIELD INFANT SCHOOL

E-Safety Policy

(Also see Computing Policy)

	Date	Minute No.
Reviewed and Approved by Governors	**C & GP 21.03.13**	**5**
Reviewed and Approved by Governors	**C & GP 22.01.15**	**16**
Reviewed and Approved by Governors	**C & GP 23.01.17**	**17**
Reviewed and Approved by Governors	**Curr. 24/01/2019**	**11**
Reviewed and Approved by Governors	_____	_____
Reviewed and Approved by Governors	_____	_____
Reviewed and Approved by Governors	_____	_____
Reviewed and Approved by Governors	_____	_____
Reviewed and Approved by Governors	_____	_____
Reviewed and Approved by Governors	_____	_____
Reviewed and Approved by Governors	_____	_____
Reviewed and Approved by Governors	_____	_____

Sladefield Infant School E-Safety Policy

Our E-Safety Policy has been written by the school, building on the Birmingham BGFL policy and government guidance. It has been agreed by the School Leadership Team and approved by Governors. It should be recognised that E-Safety is a whole school issue relating to Child Protection and not specifically an issue of Computing.

Aims

Sladefield Infant School aims to create a safe educational environment through the effective and appropriate use of digital technologies that prepares children aswell as adults, to be digital citizens of the 21st Century.

The Aims for Internet Use

Benefits of using the Internet in our school include:

- access to world-wide educational resources including museums and art galleries;
- 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 LEA and DfCSF;
- mentoring of pupils and provide peer support for them and teachers;
- opportunities for supporting individual learning needs;
- involvement of parents and children through clubs , workshops
- improved community access to school information through the school website, school text messages, TV screens in the conservatories and parent workshops.

Logons and Passwords

All users of the school Network will have individual Logon names and passwords. Logons and passwords must only be used by the intended person and never shared. Users will also have a range of other logons and passwords for systems and software. It is the user's responsibility to ensure that this information is kept secure. Misuse of accounts by others could be tracked back .It is therefore imperative that class logons are solely for the use of individual classes and any misuse will be investigated. Children in Foundation and Key Stage 1 should be taught about keeping their passwords and logons a secret, through discrete E- safety lessons throughout the year .

Use of Hardware

All school equipment belongs to the school and may not leave the building without specific permission. The use of personal equipment in school is not permitted without the specific permission of the Head Teacher or Computing Lead.

To prevent any breach of data staff memory sticks and laptops are encrypted.

On no account should repairs to computers be undertaken without the permission of the Computing Lead. It should also be noted that software should not be added or downloaded on to machines without the permission of the Computing Lead.

The Use of the Internet to Enhance Learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable such as Kiddle and what is not, and given clear guidelines for using these resources. This will entail the teacher checking what the children have typed in the search engine before clicking on the link. This is to ensure children are appropriately using the computer.
- Internet access will be planned to enrich and extend learning activities, through safe learning platforms such as Purplemash. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should review websites used prior to teaching to ensure they are suitable so that they can guide pupils safely to 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 and how to report inappropriate behaviour whilst they are online. E-Safety lessons will be taught as discrete lessons throughout the year as part of PHSE lessons.

Evaluation of Internet Content

- With regards to safeguarding issues, if staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing Lead /Head teacher.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with recent GDPR copyright law (See appropriate policies for more information).
- Key Stage 1 Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Ongoing training will be available to staff in the evaluation of Web materials and methods of developing children's critical attitudes.

Monitoring the policy

The school will monitor the impact of the policy to all members of the school community using

- Monitoring logs of internet activity
- Surveys / questionnaires / individual class newsletters
- CPOMS – E Safety incidents reported

Management of E-mail

- Pupils and staff may only use approved e-mail accounts (Bgfl 365 logins issued by the ICT technician) on the school system.
- Pupils and staff must immediately tell a teacher if they receive offensive e-mail.
- Pupils need to be aware that they must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Each class will have its own Twitter account which will need to follow specific guidelines before posting tweets. This will be at the discretion of the class teacher, but overseen by the Deputy Head.
- Access in school to external personal e-mail accounts and social networking sites must be avoided to prevent spam being picked up by Policy Central.
- E-mail sent to an external organization should be written carefully and formally addressed in a professional manner.
- The forwarding of chain letters is not permitted.

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 Head Teacher/ Deputy Head 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 and new GDPR laws (see appropriate policy).
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

The Use of Social Network sites and Newsgroups

- The Use of Social Network and newsgroup sites will not be made available to pupils unless an educational requirement for their use has been demonstrated.

The Safe Use of Chat Rooms

- Anyone within the school environment will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments e.g. www.gridclub.com, skyping. This use will be supervised and the importance of chat room safety emphasised following government guidelines.
- A risk assessment or perception survey will be carried out before pupils are allowed to use a new technology in school.

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.

Authorisation of Internet Access

- The school will keep a record of all staff and pupils who are not permitted to use the Internet.
- In Reception and Year 1, access to the Internet will be by adult demonstration with some directly supervised access to specific, approved on-line materials.
- Year 2 pupils will be given opportunities to work with a greater independence but will still require some adult supervision, only after understanding and accepting the internet use agreement and being taught about responsible use. As a safer way of researching children will use Kiddle when researching rather than other search engines such as Google or Bing.
- During induction meetings, parents will be able to choose if they want their child's photo on the school website or displayed in school.
- When and where appropriate, pupils will be issued class email accounts when its use is planned into the curriculum. The use of e-mails will be under supervision and only to individuals arranged by the teachers.
- **Pupils must be taught never to enter any 'live' information about themselves on the Internet or through e-mail. This includes name, address, telephone number, school, friends, pets etc.**
- **Pupils may not upload photos onto the Internet. This should only be done by staff.**
- Pupils should be taught never to arrange to meet anyone through the Internet.

Staff and pupils must recognise that their Internet and e-mail usage is monitored by the school (this includes usage of digital devices taken off-site ie laptop, computer).

Internet usage should not be in breach of copyright law and adults using it should not do anything which exposes children to danger.

All users must be aware that they should not visit Internet sites, make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to: pornography (including child pornography, promoting discrimination of any kind, promoting racial or religious hatred, promoting illegal acts, breach any LA/School policies e.g. gambling, do anything which exposes children to danger or any other information which may be offensive to colleagues.

Mobile Phone, Cameras and Video Usage

New and emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Images /films of children should be stored on the schools' network and encrypted laptops/memory sticks only. Each member of staff has the responsibility of deleting the images when they are no longer required, or the pupil has left the school. It is imperative all staff comply with new GDPR laws about data protection and copyright issues.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on trips. Personal mobile phones are not permitted to be used in school unless permission is given from the Head Teacher.

All users should be taught that they may not give their mobile number/address to anyone who is not a friend. They should also be taught that messages should be respectful and if they receive any message or content they are uncomfortable with they should report it immediately to an adult.

If it is discovered that users have inappropriate content on their phones the Head teacher has a right to confiscate the device and approach the parents and the police if necessary.

Policy Central

Sladefield Infant School has Policy Central software running on the Network. This software has been installed in-line with City and Audit recommendations. Policy Central monitors both keyboard (in any application) and internet activity. It continually scans for keywords and images which are possible indications of: inappropriate internet usage, pornography, grooming or other Child Protection issues. The software will store possible breaches in appropriate use on a secure server in the City. Access to these screen shots will only be by the Deputy Head, who will decide if screen shots are 'false-positives' or need further investigation. Further investigations will need to be directed to authorities within the City.

It is essential that children/student/staff within the school are aware that their activities on the Internet and school Network are monitored in this way. It is the duty of school staff to inform them of this issue. Where children have used such digital devices inappropriately whether at home or in school, teachers or other school staff can record their concerns on CPOMS. This will be closely monitored by the Computing Lead and the SLT Team.

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 by using safe engines like Kiddle. 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 LEA can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimize risks will be reviewed regularly.
- The Head Teacher and Governors will ensure that the Internet policy is implemented and compliance with the policy monitored.

Management of Filtering

- The school will support BGFL's filtering policy (see appendix)
- The school will work in partnership with parents; the LA, DfCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- Computers/ laptops or any other digital devices from home must not be used through the schools network or via a dial up internet provider as they will not follow the schools filtering or virus protection system.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing co-coordinator, head teacher or the ict technician.
- The Deputy Head will ensure regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- **Any material that the school believes is illegal must be referred to the Head Teacher who will inform the Internet Watch Foundation/Central Policy (please see references given later).**
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

Pupil Consultation

- **Rules for Internet access 'THINK THEN CLICK' will be posted in all rooms where computers are used**.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- There will be a greater emphasis on E safety which will be prevalent within the New Computing planning and workshops for parents.

Staff Consultation

- All staff must accept the terms of the 'Responsible Internet Use' statement and 'Birmingham Education Service Policy for Acceptable use of the internet' before using any Internet resource in school. Staff will be asked to sign a School Contract relating to Computing usage. (See appendix)
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained when given the school handbook.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by the Senior leadership team.
- Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.

Maintenance of Computing System Security

- The school computing systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the LEA, particularly where a wide area network connection is being planned.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media such as floppy disks, memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The Computing co-coordinator / network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

Internet Use and Complaints

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Sanctions available include:

- removal of Internet or computer access for a period;
- informing parents or carers;
- interview/counseling by Head Teacher/police

Parental Support

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure, and workshops 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.
- Interested parents will be referred to organisations such as PIN, Internet Matters and NCH Action for Children (URLs in reference section) as well as providing parental workshops.

Internet use by the Community

- All adult users will need to read and sign the 'Birmingham Education Service Policy for Acceptable use of the internet' and sign the acceptable use sheet (see appendix).

Health and Safety

- Desk and floor space around workstations should be free of bags and coats, and gangways and exits should be kept clear at all times. All digital devices are Pat tested yearly and loose wires checked as well as digital devices switched off to prevent them overheating.
- When using the computers for longer periods of time, chairs should be used which have back rests, so allowing the user to lean back occasionally, away from their work, which is particularly important in Computing areas to avoid eye strain?
- Users should know how to adjust a screen for brightness and contrast, and how to position it to avoid glare from lights or windows.
- Users should be looking down at the screen, with the top of the screen roughly at their eye level.
- There is a very slight risk of triggering epileptic seizures from excessive screen flicker – there is wide variation in the 'steadiness' of screen image from one

monitor to another. If an individual child is at risk then consultation should be made with the relevant therapist or doctor.

- Pupils should take a break from the computer at least once every twenty minutes, and should do some simple stretching exercises to relieve the muscles they have been using, for example their hands, wrists and neck.
- Pupils sharing a computer should be encouraged to make sure that everyone in the group can see without straining.

Review Date: January 2019 by H. Hanif (Computing Lead)

Sladefield Responsible Internet Use letter to parents

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, Sladefield Infant School is providing supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use Internet at school.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and we can provide references to information on safe Internet access if you wish. Whilst every effort is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.
Should you wish to discuss any aspect of Internet use please telephone me to arrange an appointment.

Yours sincerely

(Head Teacher)

Sladefield Responsible Internet Use Agreement

Responsible Internet Use
Please complete, sign and return to the school secretary
Pupil:
Form:

Pupil's Agreement
I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.
Signed: Date:

Parent's Declaration and Understanding of Internet Access
I have read and understood the school rules for responsible Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.
Signed: Date:
Please print name:

Parent's Consent for Photographs
I agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used. If work is displayed on the Website it will only be identified by the children's initials and with their permission.
Signed: Date:

References

Particularly for Parents and Children

National Action for Children (NCH) www.nchafc.org.uk/itok/
Parents Guide on Internet usage

Bullying Online www.bullying.co.uk
Advice for children, parents and schools

FKBKO - For Kids by Kids Online www.fkbko.co.uk
Excellent Internet savvy for kids; KS1 to KS3

Parents Information Network (PIN) www.pin.org.uk
Comprehensive guidelines on Internet safety

Parents online www.parentsonline.gov.uk/2003/parents/safety/index.html
Interactive learning and safety advice, excellent presentation for parents.

Kidsmart www.kidsmart.org.uk
An Internet safety site from Childnet, with low-cost leaflets for parents.

Think U Know? www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

Family Guide Book (DfCSF recommended www.familyguidebook.com
Information for parents, teachers and pupils

NCH Action for Children www.nchafc.org.uk
Expert advice for children, young people and parents.

Safekids www.safekids.com
Family guide to making Internet safe, fun and productive

Particularly for Schools

Associations of Co-ordinators of IT (ACITT)
Acceptable use policy for the Internet in UK Schools, original straightforward text.
www.g2fl.greenwich.gov.uk/acitt/resources/assoc/aup97.doc

NAACE / BCS www.naace.org (publications section)
A guide for schools prepared by the BCS Schools Committee
and the National Association of Advisers for Computer Education (NAACE)

DfCSF Superhighway Safety http://safety.ngfl.gov.uk
Essential reading, both Web site and free information pack. Telephone: 0845 6022260

KS2 Internet Proficiency Scheme
www.becta.org.uk/corporate/corporate.cfm?section=8&id=2758
A Becta, DFCSF and QCA pack to help teachers educate children on staying safe on the internet

Internet Watch Foundation - www.iwf.org.uk
Invites users to report illegal Web sites

Data Protection www.informationcommissioner.gov.uk/

New Web site from the Information Commissioner
Kent Web Skills Project **www.kented.org.uk/ngfl/webskills/**
Discussion of the research process and how the Web is best used in projects.
Click Thinking: Scottish Education Department **www.scotland.gov.uk/clickthinking**
Comprehensive safety advice
Copyright **www.templetons.com/brad/copymyths.html**
Irreverent but useful coverage of the main aspects of copyright of digital materials, US-based.
Internet Users Guide **www.terena.nl/library/gnrt/**
A guide to network resource tools, a book (ISBN 0-201-61905-9) or free on the Web.
Alan November – The Grammar of the Internet **www.edrenplanners.com/infolit/**
Article explaining how to evaluate Web sites and information
DotSafe – European Internet Safety Project **http://dotsafe.eun.org/**
A comprehensive site with a wide range of ideas and resources, some based on Kent work.
Cybercafe **http://www.gridclub.com/home_page/hot_headlines/cyber.shtml**
Internet proficiency through online games for KS2, with a free teacher's pack.

Sladefield Infant Acceptable Use Policy

1. Introduction

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 of the guidelines have been produced in the light of current legislation including the following Acts.

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

Aim
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.

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

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.

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.

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. RESPONSIBILITIES

SLT
The policies and these guidelines have been approved and adopted by the Senior Leadership Team.

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

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).

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.

3. MAIL GUIDELINES

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.

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 emailed 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.

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.

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.

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.

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.

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.

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.

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.

4. INTERNET GUIDELINES

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.

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.

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.

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.

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.

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.

Sladefield Infant Filtering Policy

Safeguarding web pages and e-mail
A key element of the Birmingham Grid for Learning is that it is a "filtered" service. It is important that access to the Internet is controlled and monitored, and that access to inappropriate sites is blocked.

Web filtering
Since the beginning of September 2001 the filtering software used on BGfL has been supplied by N2H2. Further information on N2H2 can be obtained from the N2H2 web site.
All access from the Grid to the Internet has to be made through the filtering server which runs N2H2. In order to deliver Internet access at the fastest possible speed to schools, this filtering service now offers a standard level of filtering across all schools.

The following categories of site are blocked:

- Pornography
- Strong and offensive language
- Violence
- Chat rooms/Social network sites - ie facebook
- Adults only
- Drugs (sites that promote or advocate recreational drug use)
- Personal (dating)
- Gambling
- Hate/discrimination
- Tasteless/Gross
- Weapons

In addition, some sites not in these categories are also blocked, for example the World Wide Wrestling federation site, Sparklebox following many requests from schools.
It is possible for schools to have their own local filtering server, which will give some additional control over access to the Internet. This will include being able to set access levels by person, computer and time of day, giving total control of what can and cannot be accessed on the Grid or Internet. For more information on school based filtering, e-mail connectivity@bgfl.org. Central Policy automatically filters emails and web searches.
If you have any comments on the filtering policy, or would like to suggest sites which should be blocked but aren't, or sites which should not be blocked but are, please e-mail filtering@bgfl.org

E-mail filtering
We also use software to filter e-mail, to ensure that file attachments containing computer viruses cannot be sent or received, and to ensure that e-mail is not used in an inappropriate way. It is possible to check for inappropriate words or phrases in e-mails, and to divert them if required.
The software used for this purpose is called Mailsweeper, supplied by Content Technologies.
Use of the e-mail service on BGfL is subject to the Birmingham City Council policy on the acceptable use of e-mail.
This software is also used to direct e-mail to the right place on the Grid, for example to a school's own mail server, or to the BGfL web server.

Agreement for Loan of Laptop Computer

As part of the School Improvement Plan for Sladefield Infant School it has been agreed to provide laptop computers for designated members of the teaching staff. It has also been agreed that one of these computers should be assigned to _____, and Sladefield Infant School hereby agree as follows:

1. The laptop computer identified below shall be loaned to (the above named) for his/her personal use. The loan shall terminate when (the above named) ceases to be employed at Sladefield Infant School, unless the School deems the loan to be terminated by breach of conditions in which case it will terminate forthwith. On the termination of the loan, the laptop computer shall be returned to the School.

2. (The above named) has not previously been in receipt of any computer equipment funded by Government grants. Although the school may from time to time fund laptops for teachers without the Government grant.

3. The laptop computer is covered by insurance provided by Sladefield Infant School except for loss, theft or damage occasioned by the negligence of (the above named), such as leaving the laptop prominent in an unattended car, in which case any such loss or damage shall be made good at the expense of (the above named). (The above named) is aware of the level of risk s/he undertakes by virtue of this insurance cover.

4. (The above named) agrees to abide by Birmingham City Council and Sladefield Infant School's policies in respect of observance of requirements in respect of the Data Protection Act 1998 (see http://www.bgfl.org/services/editdata and http://www.dataprotection.gov.uk/), in particular the specific requirements under the Act imposed by the School's registration with the Information Commissioner.

5. In practice this means that teachers should refrain from using, on their laptops, information about identifiable individuals: if they do (e.g. assessment data exported from SIMS or Facility), they need to exercise great care in keeping their work under a secure user password, which is not known to other users of the laptop such as family members. *Please see acceptable use of computer networks (including the Internet and the Birmingham Grid for Learning) (see http://www.bgfl.org/services/lft/resp-netpolicy.htm),health and safety of (the above named) or any other individual (see http://www.bgfl.org/services/lft/resp-health.htm). (The above named) will in addition take all reasonable steps to ensure that any other user of the laptop will also abide by these requirements.*

6. (The above named) agrees to pay any telephone or telecommunication charges incurred in connecting the laptop computer to private or public networks, except in the case of

connection to the Local Area Network of any school in connection with professional duties. (The above named) understands that the supply and use of consumables used at home are the teacher's responsibility.

7. In the event of the laptop requiring repair, (the above named) will return the laptop computer to Sladefield Infant School for collection and repair by the supplier and will arrange for such collection and repair. (The above named) undertakes not to attempt any such repair him/herself. In this event, (the above named) agrees that software repair may be limited to restoration of the computer's original software image and therefore that responsibility for regular backup of data and validation of backups rests with (the above named). Sladefield Infant School ICT staff will facilitate such backups and validation, for example by appropriate connections to the school's Local Area Network.

8. (The above named) undertakes not to install any software on the laptop computer without the written sanction of Sladefield Infant School. (The above named) further undertakes not to install any Internet Service Provision (other than that provided with the laptop computer) without the written permission of Sladefield Infant School which shall not be granted without consultation with appropriate officers of Education IT Services. (The above named) will ensure that the laptop anti virus software is regularly updated and will cooperate in maintaining the Sladefield Infant School antivirus policy. (The above named) will produce the laptop if requested by Sladefield Infant School for anti-virus checking and updating if required to do so.

9. (The above named) and Sladefield Infant School agree that the teacher must use the laptop computer primarily be for the teacher's personal and professional development in connection with her/his duties in the school, and that both parties shall collaborate in recognising what activities might produce outcomes beneficial to both the teacher and the school. To this end, Sladefield Infant School will endeavor to provide any training mutually agreed to be necessary. Both parties agree to provide
any information requested by Birmingham City Council officers, the Department for Education and Skills, the Office for Standards in Education, National College of School Leadership, or other comparable agency, in investigating the effectiveness and value for money of the Laptops for Teachers Initiative.

Schedule of Loan:
Laptop Computer – Make/model: ……
Serial number: ……
Signature ……..
Date ……
Returned and Checked by: (print name) Reason for return: ……..
Signature (of checker)……
Signature (of returner)……

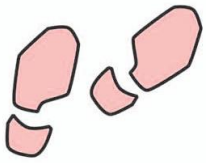
These rules help us to stay
safe on the Internet

Think then Click

We only use the Internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.



We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

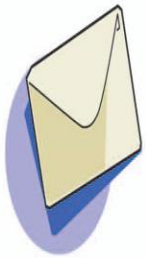
Think then Click

We ask permission before using the Internet.

We only use websites our teacher has chosen.

We immediately close any webpage we don't like.

We only e-mail people our teacher has approved.

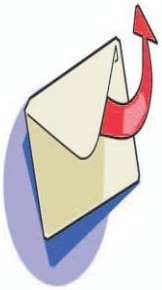


We send e-mails that are polite and friendly.

We never give out a home address or phone number.

We never arrange to meet anyone we don't know.

We never open e-mails sent by anyone we don't know.



We never use Internet chat rooms.

We tell the teacher if we see anything we are unhappy with.