Internet Policy for Parents and Pupils

Why is Internet use important?
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.
This policy will help to protect pupils from undesirable experiences or materials when using the Internet

How does the Internet benefit education?
Benefits of using the Internet in education include:

- access to world-wide educational resources;
- educational, social and cultural exchanges between pupils world-wide;
- peer support and mentoring of pupils and teachers;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- exchange of curriculum and administration data with the Local Authority (LA) and Department for Education (DfE);
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- Independent learning opportunities.

How will Internet use 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 and what is not and given clear objectives for Internet use.
- Pupils will learn to evaluate 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.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will e-mail be managed?

- Pupils in the teaching centres will be provided with an email account, for other areas of the school it is by the request of the Head of Sector
- Pupil email accounts may be withdrawn by the Heads of Sector if the student is considered to be a risk. Sectors must carry out a risk assessment prior to this request.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail/msn.
- 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 at Key Stage 2 and below.

Social Networking Sites

- Social networking, e.g. Facebook/Twitter/MSN sites should not be accessed during school hours. Some of our students are not legally old enough to use these, i.e. Facebook has an age restriction of 13.
- Any inappropriate or offensive comment to, or about, another student in school will be treated in line with the school bullying policy.

- Pupils should take a screen shot to evidence any inappropriate or offensive comments.

How should Web site content be managed?

- The point of contact on the Web site will be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Permission to use a child's photograph will be obtained from parents/carers prior to its use.
- Pupils' full names will not be used anywhere on the website.
- Written permission from parents or carers will be obtained on admission to enable photographs of pupils to be published on the school Web site.

What are newsgroups and e-mail lists?

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

Can Chat be made safe?

- 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.
- Any internet chat can be monitored.

eSafety

- The school will deliver a full esafety program to students to raise awareness of safety issues such as grooming, online gambling, pornography, etc. This will be carried out in conjunction with CEOPS and other esafety organisations.

The School use Policy Central software to monitor internet usage. A member of staff in each sector will monitor that sectors usage. Any concerns will be handled in line with the school child protection policy.

- The school will have a designated member of staff for esafety, and a designated Senior Information Risk Officer (SIRO).
- The school will make available esafety resources to parents, including advice on software.

How can emerging Internet applications be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and other portable devices, will not be used during lessons or formal school time unless under the direction of a member of staff. The sending of abusive or inappropriate text messages is forbidden.

System Security

- Each person is responsible for their individual use. If you are away from your computer, you are expected to lock it.
- Each person must not give account or password information to another user or allow another user to utilise their account.
- Users will immediately notify someone if a possible security problem is identified. Do not go looking for security problems because this may be construed as an illegal attempt to gain access.
- Users will not install or download any software programs without the permission of the ICT department, or alter the schools' software in any way.
- Students will not open any email or attachment that is from someone you do not already know without the permission of school staff.

How will Internet access be authorised?

- The school will keep a record of any pupils whose parents have specifically denied internet or e-mail access.

Primary

- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- At Key Stage 2 Parents will be informed that pupils will be provided with supervised Internet access.

Secondary

- By using the Internet, secondary students are agreeing to abide by the Responsible Internet Use statement.

Hospitals.

- Parents will be asked to sign and return form stating that they have read and understood the Acceptable Use document.

How will the risks be assessed?

- 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 Birmingham Local Authority can accept liability for the material accessed, or any consequences of Internet access.

How will filtering be managed?

- 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 Birmingham City Council using the email filtering@bgfl.org via the E-Safety coordinator

How will the policy be introduced to pupils?

- Rules for Internet access 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.
- KS3 pupils will be taught safe use of the internet during ICT lessons

Your Rights?

- Be aware the contents of your personal files on the school computer system, including email and messaging are monitored.
- Routine maintenance and monitoring of the school computer system may lead to discovery that you have violated this policy.
- An individual search will be conducted if there is reasonable suspicion that you have violated this policy. The investigation will be reasonable and related to the suspected violation.

How will ICT system security be maintained?

- 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 Local Authority when new installations or initiatives are being planned.

How will complaints regarding Internet use be handled?

- Responsibility for handling incidents involving pupils will be delegated to the appropriate Head of Sector.
- Any complaint about staff misuse must be referred to the Principal.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School Internet Policy in the admission pack and on the school Web site.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Parents are provided with cybersentinel logins, to monitor useage or internet at home, if they want it.

What does the school deem to be inappropriate or undesirable material?

- The obscene, offensive, illegal or inaccurate.

- Pupils should not feel or become uncomfortable, threatened or worried by material or information on websites or from e-mail.
- Similarly pupils must not harass, insult, attack others, violate copyright, or trespass in others' folders.

Protecting children

- The school will never publish photographs of, or name, individual children. It will be careful to only publish photographs of groups of pupils and only describe them as such (e.g. Children investigating a science problem).

LA Policy

- All internet use in the school will be governed by Birmingham City Council's Acceptable Use Policy and the School's Acceptable Use of the Internet Policy for pupils and staff

Copyright

- Copyright of material will be respected by all users of the school network.
- The school respects the IPR (Intellectual Property Rights) of pupils' work and will gain permission before any is published on the school website of BGfL.

Action taken following inappropriate conduct

- Minor infringements will be reported to the appropriate Head of Education and could result in restricted internet access for the pupil thus preventing a repeat of the incident.
- Any pupil, who deliberately breaks these rules, will not be allowed to use the Internet or computers while the incident is being investigated.
- Once the incident has been investigated it is the responsibility of the appropriate Head of Sector to take action in line with the School's Disciplinary Policy.
- When there is evidence of a criminal offence, both parents and the police will be informed.
- The school reserves the right to block internet sites and or pupil usage if it is believed to be detrimental to learning.

School/home Internet user agreement

- The school will require a signed agreement from parents before allowing pupils to use the internet.

Due to the ever changing nature of ICT, and CEOP developments, these policies may be updated more often than other policies. Therefore after initial approval any amendments will be agreed by the governor's curriculum committee. The policy will continue to be reviewed by full governors as per the calendar.

Please cross reference to Anti-Bullying and Anti-Harassment Policy for Pupils

References

Particularly for Parents and Children

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

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.

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

Notes on the legal framework

This page must not be taken as advice on legal issues, but we feel that schools should be alerted to some of the legislation that may be relevant.
The Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day to day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

Schools could start by banning private use of a school's computer system, but then allow private use following application to the Principal. The Rules for Responsible Internet Use, which every user must agree to, contain a paragraph that should ensure users are aware that the school is monitoring Internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring.

The following legislation is also relevant:

Data Protection Act /98 concerns date on individual people held on computer files and its use and protection.

Copyright, Design and Patents Act 1988 makes it an offence to use unlicensed software

The Telecommunications Act 2003 Section 43 makes it an offence to send offensive or indecent materials over the public telecommunications system.

Protection of Children Act 1999

Obscene Publications Act 1959 and 1964 defines "obscene" and related offences.

References:

Brief introduction to dangers and legal aspects of the Internet.
www.bbc.co.uk/webwise/basics/user_01.shtml

HMSO: Full text of all UK legislation and purchase of paper copies.
www.legislation.hmso.gov.uk

Agreement

James Brindley School

Responsible Internet Use

Please complete, sign and return this section to the school clerical assistant

Pupil:	***Sector:***
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 Agreement for Internet Access I have read and understood the school rules for responsible Internet use. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials at school. 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 ICT facilities. I agree that internet access should be allowed in this instance.	
Signed:	***Date:***
Please print name:	

THESE ARE THE REASONS WHY I MUST COMPLY WITH THE COMPUTER NETWORK POLICY AT JAMES BRINDLEY SCHOOL.

I agree to keep the rules

concerning being safe on computers in school, when I became a pupil at JBS.

I agree to this every time I use the internet at school.

I have been taught what an inappropriate use of the internet is.

If I discover sites I know are unsafe yet are not blocked I must tell staff immediately

so that they can protect me and my friends.

I agree not to install or download any software or programs

or alter the schools' software in any way.

This includes transferring data from home to school.

Viruses can easily be transferred from one computer system to another

causing long-term and expensive damage to the school network

and also disrupting the education of all pupils.

I know everything I do on the JBS computer network is monitored.

Both my centre staff and the ICT Technicians do this to keep me safe.

If I break these rules I know that my computer access will be restricted

whilst the incident is being investigated,

followed by a time to make sure that I and my parents

understand why this has happened.

The school has this right and **I have agreed to this.**

Using the computer network is only for pupils

who show a responsible and mature approach to its use.

Therefore as I do not want to lose this privilege I will keep the rules.