ICT Acceptable Use policy and Cyber safety policy

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- iPads, iPods, Tablet pc's
- Mobile - Smart phones with text, video and web functionality
- Other mobile and wireless devices

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At The British International School of Jeddah (BISJ), we understand the responsibility to educate our students on Cyber-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain safe when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on students, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for our school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreements (for all staff, students and parents) are inclusive of both wired and wireless internet; technologies provided by the school and technologies owned by students and staff, but brought onto school premises.

Passwords and Password Security

Users are provided with an individual network username and password that must be used to access any computer or wireless services.

Users should:

- Change passwords whenever there is any indication of possible system or password compromise.
- Use a strong password (a combination of upper and lower case letters, symbols and numbers – the longer your password, the safer it will be)
- Not record passwords on paper or in an unprotected file.

Staff must make sure that workstations are not left unattended when logged in, unless it is locked by the user or password protected screen saver.

Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk especially to young and vulnerable people. In school, all use of the internet is logged and monitored. Any inappropriate use will be reported and dealt with in line with this and other school policies.

It should be noted that:

- The school internet access is provided for educational use primarily, and all users should be mindful that it is a shared resource.
- All internet activities including access to social media will be regulated.
- Staff will preview any recommended sites and evaluate the educational value before promoting the use of these sites by students.
- All users must observe software copyright at all times. It is against school policy to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources and be critical about information published on the internet – not all sources are reliable.

Managing E-Mail

The use of e-mail is an essential means of communication for staff, students and parents. All users are aware that e-mail should not be considered private.

We recognise that students need to understand how to style an e-mail in relation to their age and good network etiquette; "netiquette". Students are introduced to e-mail as part of the ICT scheme of work.

- The school provides all staff and students from Year 3 to IB with their own e-mail account to use for all school related business and school work. The use of school provided email minimise the risk of receiving unsolicited or malicious e-mails at school and avoids the risk of personal information being revealed.
- Staff and students must use private email for non-school related and private communication.
- For the safety and security of users and recipients, all mail is screened by anti-virus and anti-spam software, filtered and logged.
- All users are discouraged from conducting school business using personal e-mail addresses.
- Think before you send! All e-mails should be written and checked in the same way you would if it was a letter written on school headed paper.
- Keep the number and relevance of e-mail recipients, particularly those being copied to management, to the minimum necessary and only when appropriate.
- Whole School emails should be only for school related business. Any other whole school messages must be approved by the Head Teacher prior to distribution of the message.
- All users are expected to check school e-mail regularly.
- All users must actively manage their e-mail account by deleting all e-mails of short-term value and frequent house-keeping on all folders and archives including saving and removing attachments.

- The forwarding of chain letters is not permitted in school.
- All users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language, not revealing any personal details about themselves or others in e-mail communication.
- All users must immediately inform a staff member or management if they receive an offensive or inappropriate e-mail.

Protecting Personal, Sensitive or Confidential Information

- Ensure that any school information including personal, sensitive or confidential information accessed from your own electronic device or stored on removable media equipment is kept secure.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.
- Ensure the accuracy of any personal, sensitive and confidential information before disclosing the information to authorised persons only.
- Ensure the security and safekeeping of any hard copies of personal, sensitive and confidential information contained in documents. This is particularly important when shared copiers, fax machines or scanners are used.
- Only download personal data from systems if expressly authorised to do so by management.
- You must not post personal, sensitive or confidential information on the internet or social media, or disseminate such information in any way that may compromise its intended restricted audience.
- E-mailing personal, sensitive or confidential information is not recommended and should be avoided where possible.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive or confidential information.
- Ensure that you are not displaying your screen on the interactive whiteboard when accessing personal, sensitive or confidential information.

Safe Use of Images

Digital images and video are easy to capture, reproduce and publish and therefore, misuse. It is not always appropriate to take or store images of any member of the school community or public, without seeking consent and considering the appropriateness.

School related images or video should be stored on the school's network and rights of access to this material will be restricted to staff and were appropriate to students directly concerned with the specific images or video.

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.
- Ensure that all ICT equipment provided by the school is kept physically secure.
- Do not attempt unauthorised access or make unauthorised modifications to any ICT equipment, programs, files or data.
- All school related data is the intellectual property of the school, and a copy of this data should be stored in the appropriate network drives provided.
- Privately owned ICT equipment should only be used on the wireless network provided for internet access.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media are checked for viruses and malware by school-provided anti-virus software – users should not interrupt this process and should ensure that the virus check is completed properly before using these files.
- Users should allow time for regular system and anti-virus update notifications.
- If you suspect there may be a virus on any equipment, stop using the equipment and contact the IT Department immediately.

Monitoring

- The IT Department is responsible for all school owned ICT equipment and may inspect or update any equipment without prior notice.

- All school ICT equipment may be monitored and logged. All monitoring, surveillance or investigative activities are conducted by IT Department staff.
- All internet activity is logged and these logs may be monitored by authorised staff and may be provided to management when requested.

Breaches

- Any policy breaches, unauthorised use or suspected misuse or abuse of ICT must be immediately reported to School Management and the IT Department.
- A breach or suspected breach of policy may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.
- Any policy breach is grounds for disciplinary action in accordance with the School's Disciplinary Procedures.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The incident must be reported to the supervising staff member and the IT Department.
- Deliberate access to inappropriate materials or misconduct by any user will reported and handled according to the School's Disciplinary Procedures.

Parental Involvement

We believe that it is essential for parents to be fully involved with promoting Cyber-Safety both in and outside of school and also to be aware of their responsibilities

- Parents are asked to read through and sign the acceptable use agreements on with the student.

Cyber-Safety Policy

Preamble

BISJ is known for its student centered approach and strong values. Our mission states that we provide excellent British-style education with an international perspective, within a safe environment, where individuals feel secure, respected, valued, happy and successful.

Clearly then we are concerned that students and staff feel safe and secure in all aspects of school operations and in particular when using technology.

The school recognises that technology plays an important and positive role in our lives, both educationally and socially. Hence, the school is committed to promoting the safe use of technology by developing an understanding of its benefits and the risks. The school will develop and maintain rigorous cyber-safety practices. To this end, we aim to equip our students with the knowledge and skills to be able to use technology safely and responsibly as digital citizens.

'Cyber safety' refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones.

Aims of the Policy

The aims of this policy are to ensure that the school community is educated about how to use technology responsibly and to ensure that effective and proactive procedures and practices for both preventing and dealing with cyber misconduct are in place.

Guidance for Students
Staying Safe

- Use a strong password (a combination of upper and lower case letters, symbols and numbers – the longer your password, the safer it will be)
- Be critical about information published on the internet – not all sources are reliable.
- Don't give out any private information over the internet or through mobile phones about you, your family, friends or other people that you know.
- Think before you send! You have to think about what you are saying and how the recipient/s may feel.
- Don't hide behind a computer screen – If you wouldn't say it to their face, don't say it at all!
- Don't post inappropriate or illegal content anywhere on the internet.
- Make sure your social network profile is set to private and check all the security settings.
- Only accept friend request from people you actually know – even if it is a friend of a friend it's not a good idea to add them unless you actually know them.
- Tell your friend to ask for your permission before uploading and / or tagging a photo of you on their social networking profiles, and make sure that you do the same.
- Don't click on any links that are imbedded in emails – if you are expecting a link type the URL into your browser and go from there.

What you should do if you receive inappropriate cyber communication

In the event that cyber-misconduct does occur, the following guidance and support procedures are available to students who are recipients of inappropriate cyber communication.

- **Evidence Gathering**
  Save any emails/ text messages or take a screen shot/print-out of any content on the internet that acts as evidence.

- **Prevent continued Abuse.**
  If possible, adjust privacy settings so that further abuse is prevented.
  Adjust settings to friends only, and remove personal information that can be seen or read by the public (photos included).

- **Reporting**
  Let your close support networks such as your parents and friends know about the incident. Tell adults, parents or teachers and keep on telling until something is done. If the internet site has a reporting facility, use it to have the abuser blocked/warned.

  Use the cyber-bullying report form on the school website to report an incident. This form will be received by the school counsellor who will contact the victim.
  Report the incident to your Head of Year or to any member of staff. You can also use the cyber misconduct hotline to have immediate access to the school counselor in order to seek help and advice.

- **Action**
  If the investigation finds that a student (or group of students) has been involved in cyber-misconduct, the school will take what is considered appropriate action.

- **On-going support**
  The school will offer practical and emotional support to students involved in such cases as outlined above.

Guidance for Parents

If your child is a victim of cyber misconduct:

- Keep communication lines open. Let him/her know it's important to tell you if he/she is being victimised. Speak openly about the communication; ensure he/she knows why and how it is inappropriate.
- Remind your child to keep passwords secret and not to post any personal information on the internet (e.g. address, phone number, etc)
- Show your child how to block/delete inappropriate messages.
- Tell him/her to NEVER seek revenge.
- Report incidents to internet service providers (the company that supplies your internet e.g. STC; ZAIN)- they could restrict the perpetrators internet use.
- Should you suspect your child is a victim of cyber misconduct, inform your child's Head of Year.
- Keep a record of relevant communications.

If you suspect your child is engaging in cyber misconduct:

- Keep communication lines open and try not to be judgmental. Ask your child what is happening; ask him/her to describe the nature of the communication.
- Assist your child in understanding the seriousness and impact of his/her behavior, encourage empathy.
- Discuss, with your child ways in which you can work together to find solutions to help him/her stop this behavior.
- Listen to his/her concerns and have follow-up discussions to ensure the behavior is not continuing.

How the school addresses cyber misconduct

Guidance for Staff

Supporting the victim:

What to do if you discover a student is a victim of cyber misconduct:

- Speak with the victim and give reassurance that the person has done the right thing by telling someone. Emphasise to the person that the nature of the communication is unacceptable.
- Emphasise the need **not** to retaliate or respond to the communication. The student should never try to seek revenge. Offer advice: take 5! - put down the mouse and step away from the computer. By not reacting and taking the time to calm down, we can avoid engaging in cyber misconduct ourselves.
- Confirm the student knows the importance of keeping their password secret and tell him/her to never reply to anybody online that he/she does not know.
- Assist the student with printing or storing the evidence safely. For example: do not delete inappropriate messages they have received, print out evidence of cyber-bullying from chat rooms/Facebook etc. or take a screen shot.
- Go through with the student what information he/she has on the public domain.
- Talk to the student about what he/she should do to prevent the problem from happening again- e.g. not responding, changing contact details, blocking contacts.
- Tell the student that he/she can report the incident to Internet service providers (ISP) and or to website moderators.
- Refer the student to his/her form tutor/HoY/Deputy Head of Pastoral.

Pastoral follow up to Cyber Bullying

- Arrange to have a meeting with the student concerned and reinforce the above points with the student.
- Contact the student's parents and let them know about the nature of the cyber communication. If necessary invite them into the school for a meeting.
- Discuss with the student's parents what Internet rules they have in place at home.
- Go through 'guidance for parents' as outlined in this policy document.
- The incident should be properly recorded and investigated in the same way as a school/playground bullying incident would.
- Ask the victim to assist you with identifying the perpetrator. This may include identifying and interviewing possible witnesses.
- Once the perpetrator is identified, steps should be taken to help him/her realize the implications and seriousness of the behavior.
- Support should be offered to him/her to assist with changing behavior.

Factors to consider when determining appropriate sanctions

- Was the material widely circulated?
- The nature of the material.
- The impact on the victim.
- The motivation of the perpetrator.

Sanctions

Sanctions will be imposed in line with the school's discipline policies and procedures

Acceptable Use Agreement: Staff

ICT, the internet and mobile devices are an essential part of our daily working life in and outside of school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT in the school and also to be especially mindful of our environment and rules regulating access and use of ICT in the Kingdom of Saudi Arabia.

All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head Teacher or Director.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed "reasonable" by the school.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to students other than for use in professional situations.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal or sensitive data taken off site must be secured.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/or staff will only be taken, stored and used for professional purposes in line with school policy. Images will not be distributed outside the school network without the permission of the parent, member of staff or Head Teacher.
- I understand that all my use of the Internet can be monitored and logged and can be made available, on request, to School Management.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's Cyber-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Name …….…….…….

Signature …….…….……

Department ……. Date ……

Acceptable Use Agreements: Primary Students

Cyber-Safety Agreement

- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will keep all my passwords safe and secret (even from my best friends)
- I will only open/delete my own files and respect everyone else's work.
- I will make sure that all my ICT communications (emails, messages, shared files etc) with other children and adults are responsible, polite and sensible.
- I will only take photos, videos and recordings of other students, school staff or parents if I have asked their permission first.
- I will not deliberately look for, save or send anything that others will find rude, unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not send my own details such as my name, phone number or home address to anyone over the internet or by email unless approved by my teacher or parents.
- I will not arrange to meet someone by email or on the internet without my parent's agreement and approval.
- I know that my use of ICT can be checked and that my parents will be contacted if anyone is concerned about my Cyber-Safety.

Dear Parent

ICT including the internet, e-mail, learning platforms and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these Cyber-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the Head Teacher.

Parent signature:

We have discussed this Cyber Safety agreement and ……..…….....(child name) agrees to follow the Cyber-Safety rules and to support the safe use of ICT at BISJ.

Parent Signature ……..……..…….

Student Signature ……..……..……

Class …… Date ……

Bring Your Own Device (BYOD) Student Agreement:

Primary School Students

The British International School of Jeddah is fully committed to creating the best possible learning environment for its students and staff. The BYOD programme is an important aspect of our aims to harness the power of the Internet and further integrate 21st century technologies into teaching and learning. We also believe that allowing our students this opportunity will motivate them to take control of their learning and become life-long learners.

To participate in the programme both student and parent must read and sign this agreement, and return it to the school. We further require that parents actively reinforce the norms of cyber safety and the expectations that we have of the child at home.

We understand and agree that:

1. Any device brought to school is the child's responsibility and the school is not liable, for loss, damage, repair or maintenance (including software updates and installation).

2. Locked storage is provided in each classroom and it is the student's responsibility to ensure that it is stored there at the beginning of the day and during break times.

3. The device must be taken home at the end of every day.

4. The device will be brought to school fully charged each morning.

5. The device is for individual use and sharing is at the student's discretion.

6. Use of the device in class is solely at the discretion of the teacher and the student must fully comply with the teacher's instructions concerning its use promptly.

7. The device may only be used for educational purposes during the school day.

8. Students must ensure that their log-in details and passwords are kept secret even from their closest friends.

9. Photographs, videos or recordings can only made of any member of school staff, other students or parents with their express permission and that of a supervising teacher. This applies during the school day, planned school activities and travelling to and from home.

10. The Saudi Arabian government filters Internet provision, as everywhere else in the kingdom. However, it is still possible that children may be exposed to inappropriate content from time to time. Parents are expected to support and encourage their child's understanding of cyber-safety and responsibility.

11. The device will not be used to search for, display, store, generate or transmit illegal, prohibited, rude or offensive material at any time, in school, travelling to and from school, or at home.

12. Cyber-bullying is a serious matter. Any use of the device to communicate hurtful, aggressive or abusive messages in any form will not be tolerated no matter how intended.

13. If at any time, the student breaks this agreement, they will lose the right to bring their device to school and may face further sanctions.

Student's Signature…….……Date……

Parent's Signature……Date…….…..

Cyber-Safety Tips for Parents

Make sure that your children are aware of what cyber-bullying is to both protect themselves and others. This kind of behavior often starts as ‘a joke’ or ‘for fun’ but rarely ends this way. Cyber-bullying is already considered a serious offence in many parts of the world.

Do not allow your children to sign up to a web site or service without your express permission and without checking the website yourself first.

If you allow your child to use social media or chat sites make sure that they are using avatars and know not to give out personally identifiable information about themselves or others.

Make sure that your child understands your expectations of them and the content that you feel is appropriate for them and that which isn’t. Even when you do this you must be aware that your child will sometimes come across internet content that is inappropriate, offensive or that makes them feel uncomfortable. It is important that they have the confidence to be able to speak to you openly and that they have strategies for reacting when it happens (eg immediately closing the site, using alt-control-delete to do this if the site prevents this).

Make sure that you know how your child is using the internet and monitor this sensitively.

Upper School Student Cyber-Safety Agreement

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without permission.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring them into disrepute.
- I will respect the privacy and ownership of others' work on line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to school staff.
- I understand that if I use my personal laptop in school I am only allowed to connect to the school wireless network.
- I understand that I will only plug a USB drives or external storage device into school ICT equipment to transfer school-based work.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parents may be contacted.

Dear Parent

ICT including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of Cyber-Safety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parents and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with the Form Tutors or Heads of Year.

Please return the signed form to the school.

Student and Parent signature:

We have discussed the Upper School Cyber Safety agreement and

……..……..... (child name)

agrees to follow the Cyber-Safety rules and to support the safe and responsible use of ICT at BISJ.

Parent Signature ……..…….

Student Signature ……..……..……

Class …… Date ……

Bring Your Own Device (BYOD) Student Agreement:

Upper School Students

The British International School of Jeddah is fully committed to creating the best possible learning environment for its students and staff. The BYOD programme is an important aspect of our aims to harness the power of the Internet and further integrate 21st century technologies into teaching and learning. We also believe that allowing our students this opportunity will motivate them to take control of their learning and become life-long learners.

To participate in the programme both student and parent must read and sign this agreement, and return it to the school. We further require that parents actively reinforce the norms of cyber safety and the expectations that we have of the child at home.

We understand and agree that:

1. Any device brought to school is the child's responsibility and the school is not liable, for loss, damage, repair or maintenance (including software updates and installation).
2. The device must be taken home at the end of every day.
3. The device will be brought to school fully charged each morning.
4. The device is for individual use and sharing is at the student's discretion.
5. Use of the device in class is solely at the discretion of the teacher and the student must fully comply with the teacher's instructions concerning its use promptly.
6. The device may only be used for educational purposes during the school day.
7. Students must ensure that their log-in details and passwords are kept secret, even from their closest friends.
8. Photographs, videos or recordings can only be made of members of school staff, students or parents with their express permission and that of a supervising teacher. This applies during the school day, planned school activities and travelling to and from home.
9. The Saudi Arabian government filters Internet provision, as everywhere else in the Kingdom. However, it is still possible that children may be exposed to inappropriate content from time to time. Parents are expected to support and encourage their child's understanding of cyber-safety and responsibility.
10. The device will not be used to search for, display, store, generate or transmit illegal, prohibited, rude or offensive material at any time, in school, travelling to and from school, or at home.
11. Cyber-bullying is a serious matter. Any use of the device to communicate hurtful, aggressive or abusive messages, in any form will not be tolerated, no matter how intended.
12. If at any time a student breaks this agreement, they will lose the right to bring their device to school and may face further sanctions.

Student's Name……. Class/Tutor Group……...

Student's Signature…….. Date…….

Parent's Signature…… Date…….

Cyber-Safety Tips for Parents

Make sure that your children are aware of what cyber-bullying is to both protect themselves and others. This kind of behavior often starts as ‘a joke’ or ‘for fun’ but rarely ends this way. Cyber-bullying is already considered a serious offence in many parts of the world.

Do not allow your children to sign up to a web site or service without your express permission and without checking the website yourself first.

If you allow your child to use social media or chat sites make sure that they are using avatars and know not to give out personally identifiable information about themselves or others.

Make sure that your child understands your expectations of them and the content that you feel is appropriate for them and that which isn’t. Even when you do this you must be aware that your child will sometimes come across internet content that is inappropriate, offensive or that makes them feel uncomfortable. It is important that they have the confidence to be able to speak to you openly and that they have strategies for reacting when it happens (eg immediately closing the site, using alt-control-delete to do this if the site prevents this).

Make sure that you know how your child is using the internet and monitor this sensitively.