Internet Acceptable Usage Policy

Introduction

The purpose of this policy is to ensure that users of the Basingstoke Alliance SCITT understand the way in which the Internet is to be used. The policy aims to ensure that the Internet is used effectively for its intended purpose, without infringing legal requirements or creating unnecessary risk.

Scope

The policy applies to:

All users and administrators of the BASCITT services and/or infrastructure.

On evidence provided by the BASCITT, staff or Trainees may be disciplined if found to be in breach of the policy. At the same time, if a user's conduct and/or action(s) are illegal, the user may become personally liable.

Policy Statement

The BASCITT encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. It should not compromise BASCITT's information and computer systems nor have the potential to damage the BASCITT's reputation.

Please read this policy carefully as you will be deemed to be aware of its contents.

During school placements please ensure you obtain a copy of/and follow their school policy on the use of the Internet and on line access. Whilst training with BASCITT Trainees will be bound by the following:

1. Use of computers, email and the internet

   The email system and the internet/intranet can be extremely valuable tools in an educational context, encouraging the development of communication skills, and transforming the learning process by opening up possibilities that, conventionally, would be impossible to achieve. The use of electronic mail as a medium for paper mail replacement and as a means of enhancing communications is encouraged.

Those using the internet are expected to do so responsibly and to comply with all applicable laws, policies and procedures, and with normal standards of professional and personal courtesy and conduct.

Computers and laptops loaned to Trainees/staff/Alliance/Associate schools by BASCITT are provided to support their professional responsibilities and Trainees/staff must notify the Programme Manager of any significant personal use (see section 1.1). Reasonable access and use of the internet/intranet and email facilities is also available to recognised representatives of professional associations i.e. union officers.

Trainees/staff must not use BASCITT equipment or property for personal gain or fraudulent, malicious, illegal, libellous, immoral, dangerous, offensive purposes. Trainees/staff should not undertake IT related activities that are contrary to the BASCITT policies or business interests including accessing, downloading, storing, creating, copying or distributing offensive material (this includes but is not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).

All forms of chain mail are unacceptable and the transmission of user names, passwords or other information related to the security of BASCITT's computers is not permitted.

1.1 Personal Use

1.1.1 SCITT's internet service may be used for incidental personal purposes, with the approval of the BASCITT Programme Manager provided that it does not:

- interfere with the SCITT's operation of computing facilities;
- interfere with the user's employment or other obligations to SCITT;
- interfere with the performance of professional duties;
- is of a reasonable duration and frequency;
- is performed in non-work time;
- does not over burden the system or create any additional expense to BASCITT;
- does not bring BASCITT, its Partnership or Alliance schools or its staff into disrepute.

Such use must not be for:

- unlawful activities;

- commercial purposes not under the auspices of BASCITT;
- personal financial gain;
- personal use that is inconsistent of other BASCITT policies or guidelines.

If a Trainee/employee fails to meet these conditions for personal use, their rights to use equipment may be withdrawn. If a Trainee/ employee fails to follow this policy and other supporting procedures, this could result in disciplinary action.

1.1.2 **Use of email and internet at home**

Access to the internet from a Trainee/ employee's home using a BASCITT owned computer or through BASCITT owned connections must adhere to all the policies that apply to their use. Family members or other non-BASCITT members must not be allowed to access BASCITT's computer system or use BASCITT's computer facilities, without the formal agreement of the Programme Manager.

1.2 Security

1.2.1 BASCITT follows sound professional practices to secure email records, data and system programmes under its control. As with standard paper based mail systems, confidentiality of email cannot be 100% assured. Consequently users should consider the risks when transmitting highly confidential or sensitive information and use the appropriate level of security measure.

1.2.2 Enhancement of the base level security to a higher or intermediate level can be achieved by the use of passwords for confidential files. It should be remembered emails forwarded from another individual can be amended by the forwarder. This possibility should be considered before acting on any such mail.

1.2.3 The following should be adhered to when using e-mails:

- open mailboxes must not be left unattended;
- care should be taken about the content of an email as it has the same standing as a memo or letter. Both the individual who sent the message and/or BASCITT can be sued for libel;
- reporting immediately to BASCITT personnel when a virus is suspected in an email.

1.3. Privacy

1.3.1 BASCITT respects users' privacy. Email content will not be routinely inspected or monitored, nor content disclosed without the originator's consent. However, under the following circumstances such action may be required:

- when required by law;
- if there is a substantiated reason to believe that a breach of the law or BASCITT policy has taken place;
- when there are emergency or compelling circumstances.

1.3.2 BASCITT reserves the right, at its discretion, to review any Trainee/ employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other policies. Trainees/staff will be notified of any monitoring which will take place and the reason for it. Monitoring will be reasonable and in accordance with Data Protection and Human Rights obligations.

1.3.3 Trainees/staff should not have any expectation of privacy to his or her internet usage. BASCITT reserves the right to inspect any and all files stored in computers or on the network in order to assure compliance with this policy. Auditors must be given the right of access to any document, information or explanation that they require.

1.3.4 Use of the Trainee/ employee's designated personal file area on the network server provides some level of privacy in that it is not readily accessible by other members of staff. These file areas will however be monitored to ensure adherence to policies and to the law. The Trainee/employee's personal file area is disk space on the central computer allocated to that particular Trainee/employee. As it is not readily accessible to colleagues it should not be used for the storage of documents or other data that should be open and available to the whole staff or wider school community.

1.3.5 Managers will not routinely have access to a Trainee/ employee's personal file area. However, management information on usage size of drives or a report outlining the amount of information held on an individual's personal file area will be made available from time to time.

1.4. Email/IT Protocols

1.4.1 Users must:

- respond to emails in a timely and appropriate fashion. The system is designed for speedy communication. If urgent, the email requires a prompt response, otherwise a response should be sent within a reasonable timeframe according to the nature of the enquiry;
- not use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details;
- not abuse others (known as 'flaming'), even in response to abuse directed at themselves;
- not use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system;
- not use, transfer and tamper with other people's accounts and files;
- not use their own equipment to connect to the BASCITT network unless specifically permitted to do so and the equipment meets appropriate security and other standards. Under no circumstances is personal equipment containing inappropriate images or links to them, to be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children;
- adults should ensure that pupils are not exposed to any inappropriate images or web links. BASCITT and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. e.g. personal passwords should be kept confidential;
- not store sensitive or confidential data on their own equipment – this extends to personal cameras, mobile phones and other similar devices;
- respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner;
- not use the internet/intranet facilities or equipment to deliberately propagate any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations;

If a user finds him/herself connected accidentally to a site that contains sexually explicit or offensive material, they must disconnect from that site immediately. Such unintentional access to inappropriate internet sites must be reported immediately to their school or BASCITT. Any failure to report such access may result in disciplinary action.

1.4.2 Except in cases in which explicit authorisation has been granted by the BASCITT Programme Manager, Trainees/staff are prohibited from engaging in, or attempting to engage in:

- monitoring or intercepting the files or electronic communications of other employees or third parties;
- hacking or obtaining access to systems or accounts they are not authorised to use;
- using other people's log-ins or passwords;
- breaching, testing, or monitoring computer or network security measures;
- interfering with other people's work or computing facilities;
- sending mass e-mails. Global sends (send to everybody in the Global address book) are prohibited.

1.5. Data protection

1.5.1 The Data Protection Act 1998 prohibits the disclosure of personal data except in accordance with the principles of the Act. This prohibition applies to e-mail in the same way as to other media. Information gathered on the basis that it would be seen by specified Trainees/ employees must not be given to a wider audience. In accordance with the provisions of Article 8 of the European Convention on Human Rights, SCITT respects the right to privacy for Trainees/staff who use IT equipment but does not offer any guarantee of privacy to Trainees/ employees using IT equipment for private purposes.

1.5.2 As data controller, BASCITT has responsibility for any data processed or stored on any of its equipment. Any Trainee/ employee monitoring will be carried out in accordance with the principles contained in the Code of Practice issued by the Information Commissioner under the provisions of the Data Protection Act 1998.

1.5.3 In order to comply with its duties under the Human Rights Act 1998, BASCITT is required to show that it has acted proportionately, i.e. are not going beyond what is necessary to deal with the abuse and that the need to investigate outweighs the individual's rights to privacy, taking

into account BASCITT's wider business interests. In drawing up and operating this policy BASCITT recognises that the need for any monitoring must be reasonable and proportionate.

1.5.4 Auditors (internal or external) are able to monitor the use of the BASCITT's IT equipment and the storage of data. They are nevertheless bound by the provisions of the Human Rights Act 1998, the Data Protection Act 1998, associated codes of practice and other statutory provisions and guidance, including the Regulation of Investigatory Powers Act 2000 in respect of any activity that could be classed as directed surveillance.

2. Social networking

The purpose of this policy is to ensure:

- that BASCITT is not exposed to legal and governance risks;
- that the reputation of BASCITT is not adversely affected;
- that our users are able to clearly distinguish where information has been provided via social networking applications, that it is legitimately representative of BASCITT;
- protocols to be applied where Trainees/employees are contributing in an official capacity to social networking applications provided by external organisations.

Social networking applications include but are not limited to:

- blogs i.e. blogger;
- Online discussion forums, for example Facebook, Bebo, Myspace;
- Media sharing services for example YouTube;
- 'Micro-blogging' application for example Twitter.

2.1 Access to Social Networking Sites

There is a complete block from personal use during working time and/or using BASCITT's computer network.

2.3 Personal social networking sites

All Trainees/staff of BASCITT should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, Data Protection and Freedom of Information legislation and the Safeguarding Vulnerable

Groups Act 2006. Trainees/staff must also operate in line with BASCITT's Single Policy for Equality.

Any communications or content published on a social networking site which is open to public view, may be seen by members of the BASCITT/ school community. Trainees/staff hold positions of responsibility and are viewed as such in the public domain. Inappropriate usage of social networking sites by Trainees/staff can have a major impact on the working relationship. Any posting that causes damage to BASCITT and or Partnership/Associate schools, any of its staff or any third party's reputation may amount to misconduct or gross misconduct which could result in dismissal.

Trainees/ staff should not use personal sites for any professional activity. BASCITT reserves the right to require the closure of any applications or removal of content published by Trainees/staff which may adversely affect the reputation of BASCITT and or Partnership schools or put it at risk of legal action.

Anyone who becomes aware of inappropriate postings on social networking sites, must report it to the BASCITT Programme Manager as soon as possible. The BASCITT Programme Manager will then follow the disciplinary procedure. If a Trainee/ employee fails to disclose an incident or type of conduct relating to social networking sites, knowing that it is inappropriate and falls within the remit of this policy, then that Trainee/ employee may be subject to the disciplinary procedure.

2.3.1 **Posting inappropriate images**

Indecent images of any Trainee/employee that can be accessed by students, parents or members of the public are totally unacceptable and can lead to child protection issues as well as bringing BASCITT into disrepute.

2.3.2 **Posting inappropriate comments**

It is totally unacceptable for any Trainee/employee to discuss pupils, parents, work colleagues or any other member of the school community on any type of social networking site.

Reports about oneself may also impact on the working relationship for example if a Trainee/ employee is off sick but makes comments on a site to the contrary.

2.3.3 **Social interaction with pupils (past and present)**

Trainees/staff should not engage in conversation with pupils on any personal social networking sites and should be circumspect in personal network contact with former pupils, particularly those under the age of 18 years. This would also apply to individuals who are known to be vulnerable adults. Offers of assistance to a pupil with their studies via any social networking site are inappropriate and also leaves the Trainee/employee vulnerable to allegations being made. It would be very rare for Trainees/employees to need to interact with pupils outside of BASCITT in a social setting and by communicating with them on social networking sites, is tantamount to the same.

Adults should ensure that personal social networking sites are set at private and that pupils are never listed as approved contacts.

Adults should not use or access social networking sites of pupils.

Should a Trainee/ employee become aware of an underage person using social networking sites, (Facebook and Bebo have set it at 13 years and MySpace have set it at 14 years), then they should report this to the site operator and if that child is at their Partnership school, then this should be reported to the Programme Manager.

2.3.4 **Making Friends**

Trainees/staff should be cautious when accepting new people as friends on a social networking site where they are not entirely sure who they are communicating with. Again this may leave Trainees/ staff vulnerable to allegations being made.

2.4 **General Terms of use**

All Trainees/staff must adhere to the following terms of use of social networking applications. This includes, but is not limited to public facing applications such as open discussion forums and internally-facing applications, (i.e. e-folio) regardless of whether they are hosted on organisational networks or not. BASCITT expects that users of social networking applications will always exercise due consideration for the rights of others and strictly in accordance with the following terms of use.

Social networking applications must not:

- be used to publish any content which may result in actions for breach of contract, defamation, discrimination, breaches of copyright, data protection, breach of confidentiality, intellectual

property rights or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the BASCITT or the local authority into disrepute;

- be used for party political purposes of specific campaigning purposes as the local authority is not permitted to publish any material which 'in whole or part appears to affect public support for a political party' (Local Government Act 1986);
- be used for the promotion of personal financial interests, commercial ventures or personal campaigns;
- be used in an abusive or hateful manner;
- be used for actions that would put other Trainees/staff in breach of the Code of Conduct;
- be in breach of BASCITT's Disciplinary Policy and Single Policy for Equality.

Where individuals from partner organisations are involved and are acting on behalf of BASCITT, they will also be expected to comply with the relevant policies.

Monitoring

Placement schools will monitor and audit the use of the Internet to see whether users are complying with their policy. Any potential misuse identified by the BASCITT will be reported to the Management Board. Any breach of the policy may lead to dismissal from the programme.

Policy written: July 2014
Ratified by Management Board: July 2014
For review: July 2015