BRIGHT EDUCATION CENTRE

Sparking the Next Generation

E-Safety Policy

Policy Date May 2016

To be reviewed: June 2017

BEC-SAFETY POLICY

It is important that this policy is read in conjunction with:

- BEC safeguarding Policy
- BEC Anti Bullying Policy
- BEC Behaviour Policy

Colleagues who need to be involved in the creation, management and maintenance of this policy are:

- Centre Director
- BEC Safeguarding team.
- Tutors.

Principles

The provisions of the *Children Act 2004*[1], *Working Together to Safeguard Children*[2] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

All of the 'staying safe' aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the Centre to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the Centre physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the Centre and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements

Full title: Working Together to Safeguard Children: A guide to inter-agency working to Safegurd and promote the welfare of children:

Purposes

Although the use of ICT and the internet provide ever increasing opportunities for children to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to the risk of harm.

Apart from the risk of children accessing internet sites which contain unsuitable material, risks to the well being of children may also exist in a variety of other ways.

This policy therefore details strategies and guidance for addressing the issues of:

- Publishing digital images and information about/of students and staff.
- Keeping children safe from Internet grooming
- Keeping children safe from Cyber Bullying
- Keeping children safe from inappropriate Internet content.
- Keeping BEC staff and other adults safe.

General principles for dealing with e-Safety issues

- An environment should be encouraged where students feel confident when it comes to reporting inappropriate incidents involving the internet or mobile technology.
- The Centre makes use of an effective range of technological tools to maintain a safe ICT learning environment. (Refer to Appendix 3).
- Roles and responsibilities of staff involved are clearly designated and monitored.

Acceptable Use Policy - Publishing digital images of students and staff.

This policy covers the publishing of digital images of students and staff in paper based documents, on the Centre website It includes both still and moving images.

The Centre does not allow images of its students and staff to be published on third party websites unless written permission has been granted.

The Centre will use digital images of students and staff where it feels it is appropriate to do so. Examples of where they might be used are:

- To celebrate achievement.
- To promote the Centre and its work.
- To improve the quality of the learning experience.

When using any digital image the Centre will ensure that the person's privacy is protected. It will do this by:

- Having the student/Tutors permission to publish.
- Not publishing (either print or audio) the student's name in a way that could link the name to the image except where parental permission is obtained.
- Not publishing any personal/sensitive details.

When storing digital images within Centre they will be stored safely in a password protected area on the Centre network.

Keeping children safe from Internet Grooming

If there is concern that a child's safety is at risk because there is a suspicion that someone is using communication technologies (such as social networking sites) to make inappropriate contact with a child the concern should be reported to and discussed with the named Child Protection Officer in Centre.

If appropriate the following could be actioned:

- A decision made as to whether parents should be contacted.
- Advise the child on how to terminate the communication and save all evidence
- Contact CEOP http://www.ceop.gov.uk/
- Consider the involvement police and social care

To safeguard students the Centre

- Blocks all Chat rooms and social networking sites (that we are aware of or made aware of) except those that are part of an educational network or approved Learning Platform;
- Only uses approved and appropriate blogging or discussion sites, such as on the LGfL / approved Learning Platform and blocks others as we are made aware of them.
- Only uses approved or checked webcam sites;

Keeping children safe from cyber bullying

Bright Education Centre will not tolerate bullying, whatever form it takes.

Bullying is personally hurtful behaviour including the use of aggression with the intention of hurting another person either physically or emotionally. This often occurs on much more than one occasion, although it can be a serious one off incident. Cyber bullying is bullying through the use of communication technology like mobile phone text messages, e-mails or websites. This can take many forms for example:

- Sending threatening or abusive text messages or e.mails, personally or anonymously
- Making insulting comments about someone on a website, social networking site (eg: facebook, MySpace, Centre reunited), online diary (blog) or messaging system.
- Making or sharing derogatory or embarrassing videos of someone via mobile phone, e.mail or website (such as 'Happy Slapping' videos).

Using ICT to bully could be against the law. Abusive language or images, used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous, may contravene the *Harassment Act 1997 or the Telecommunications Act 1984.*

1. If a bullying incident directed at a child occurs using email, website, blog or mobile phone technology and is in anyway connected to the Centre
   - Advise the child not to respond to the message
   - Refer to relevant policies including e-safety/acceptable use, anti-bullying and apply appropriate sanctions
   - Secure and preserve any evidence
   - Inform the sender's e-mail service provider
   - Notify parents of the children involved
   - Consider delivering a parent workshop for the centre community
   - Consider informing the police depending on the severity or repetitious nature of offence
   - Inform the Centre Manger/ Director

2. If malicious or threatening comments are posted on an Internet site about a pupil or member of staff inform a member of SMT who will:
   - request the comments be removed if the site is administered externally
   - Secure and preserve any evidence
   - Internally investigate (following the usual procedures for investigating serious incidents as outlined in the Centre Behaviour policy) the incident and inform the Director.

The Centre should then consider:

- Sending all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
- Endeavouring to trace the origin and inform police as appropriate.

Keeping children safe from Inappropriate Internet content

Bright Education Centre:

1. Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
2. We use the pan-London Websense, Synetrix filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
3. Encourages staff to preview all sites before use [where not previously viewed and cached] or only use sites accessed from managed 'safe' environments such as the Learning Platform;
4. Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
5. Informs users that Internet use is monitored;
6. Informs staff and students that that they must report any failure of the filtering systems directly to the Centre Manager who will report to LA / where necessary;
7. Will block pupil access to music download or shopping sites as we become aware of them – except those approved for educational purposes.
8. Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
9. Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
10. Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in- line with the school behaviour management system;
11. Will refer any material we suspect is illegal to the appropriate authorities (LA / Police) once a thorough internal investigation has taken place.

Staff Expectations: Use of Electronic Equipment

These guidelines and expectations have been produced in light of advice given to the safeguarding Team on a number of recent courses they have attended. It is a complex and ever-changing area with constantly changing and expanding technologies. However, perceived misuse of electronic equipment has had severe consequences for individuals.

1. Staff must not add students, or parents as friends on their Social Media sites

2. Staff must not give their personal mobile or landline phone numbers to parents or students

3. Staff must not use their personal mobile phones inappropriately, for example whilst teaching or on duty

4. Staff must not make comments about colleagues, students or their families on Social media sites

5. Staff must ensure that content posted about them on Social media sites (by themselves or by friends/family) is appropriate to be viewed by the general public and will not bring themselves or the Centre into disrepute. Students and parents seem to be able to find ways to access personal content on such sites. This leaves staff in a very vulnerable position.

8. Staff should be aware that anything they or others have posted on Twitter is open to public access.

Appendix 1 Education and training

Students

- Regular assemblies
- Education through ICT lessons
- Posters and reminders.
- Distributing any appropriate leaflets or promotional material provided by external organisations.
- An e safety awareness day.

Staff

- Regular reminders and guidance using staff meetings, email, website
- Annual requirement to read and sign off ICT policy.

Parents and other adults

- Flagging of policies and procedures on Centre website.
- Awareness raising events.

Appendix 2 Guidance - <u>What do we do if?</u>

N. B. Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

An inappropriate website is accessed <u>unintentionally</u> in Centre by a Tutor or child.

1. Play the situation down; don't make it into a drama.
2. Report to the Centre Director and decide whether to inform parents of any children who viewed the site.
4. Inform the Network company.

An inappropriate website is accessed <u>intentionally</u> by a child.

1. Refer to the ICT policy (student guidance) and apply sanctions in line with the Centre behaviour policy.
2. Report to the ICT Department and Head of Year who will inform the parents.
3. Inform the Centre Manager

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you; do not view the misuse alone.
2. Report any suspected serious misuse immediately to the Director
3. Ensure that there is no further access to the PC or laptop.
4. If the material is offensive but not illegal, the Director should then:
    - Remove the PC to a secure place.
    - Instigate an audit of all ICT equipment by the Facility manger service providers to ensure there is no risk of pupils accessing inappropriate materials in the centre
    - Identify the precise details of the material.
    - Take appropriate disciplinary action.
    - Inform Trustee of the incident.
5. In an extreme case where the material is of an illegal nature:
    - Remove the PC to a secure place.
    - Document all action taken.
    - Contact the appropriate authorities.

A bullying incident directed at a child occurs through email, website, messaging system or mobile phone technology and is in any way connected to the Centre.

1. Advise the child not to respond to the message.
2. Secure and preserve any evidence.
3. Report to Director.
4. Apply sanctions in line with the Centre behaviour policy.

Malicious or threatening comments are posted on an Internet site (e.g. blogs or social networking sites) about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Investigate thoroughly and apply sanctions as appropriate.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child.

1. Report to and discuss with the Safeguarding Officer in Centre and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services

Appendix 3 - Technical safeguarding

This Centre

- Ensures network health through appropriate anti-virus software etc and network set-up. Pupils cannot download executable files such as .exe / .com / .vbs etc.;
- Ensures the network is 'healthy' at all times.
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows pupils access to Internet logs;
- Has network auditing software installed;
- Uses security time-outs on Internet access where practicable / useful;
- Uses individual log-ins for pupils and all other users;

applications and Internet web sites, where useful;