



# SB Mentoring

Offering a foundation for future success

## e-Safety Policy



## Rationale

New technologies have become integral to the lives of all users in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers, mentors and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. All users should have an entitlement to safe internet access at all times.

The requirement to ensure that all users can use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This school/provision e-safety policy should help to ensure safe and appropriate use.

The development and implementation of such a strategy should involve all the stakeholders in a child's education from the centre manager, classroom mentors, parents, members of the community and the students/pupils themselves.

The use of these exciting and innovative tools in provision and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put users at risk within and outside the provision. Some of the dangers they may face include:

- Access to illegal, harmful, or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy, and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files

- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other provision policies (Safeguarding policy).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build user's resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The provision must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help users (and the wider community) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

## **E-Safety Policy**

Our e-safety policy has been written by the manager, following government guidelines. It has been agreed by all staff and can be found on our website.

### **Scope of the Policy**

This policy applies to all members of the provision community (including staff, pupils, volunteers, parents/carers, visitors, and community users) who have access to and are users of SB ICT systems, both in and out of the provision.

## **E-Safety Roles and Responsibilities**

The following section outlines the roles and responsibilities for e-safety of individuals and groups within our provision.

### **Centre Manager & Deputy Manager**

- The centre manager & deputy are responsible for ensuring the safety (including e-safety) of members of the provisions community.
- The centre manager & deputy are responsible for ensuring that the IT support and other relevant staff receive suitable CPD training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The centre manager & deputy will receive regular monitoring reports from IT support.
- The centre manager & deputy should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

### **Learning Mentors**

- Take day-to-day responsibility for e-safety issues.
- Ensure that all procedures that need to be followed in the event of an e-safety incident take place.
- Complete E-Safety training yearly.
- Receive reports of any e-safety incidents and create a log of incidents to inform future e-safety developments.

### **SB Mentoring Network Provider**

- Ensure that the provision's ICT infrastructure is secure and is not open to misuse or malicious attack as well as off-site access.
- Ensure that users may only access the provisions networks through properly enforced password protection in which passwords are regularly changed.
- They keep up to date with e-safety technical information to effectively carry out their e-safety role and to inform and update others as relevant

### **All staff are responsible for ensuring that:**

- They have an up-to-date awareness of e-safety matters and of the current e-safety policy and procedures
- They have read, understood and signed the provisions e-Safety policy
- They report any suspected misuse or problem to the centre manager for investigation

- Digital communications with pupils should be on a professional level and only carried out using official provision systems.
- E-safety issues are embedded in all aspects of the curriculum.
- Pupils follow the provisions e-safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current provision policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are place for dealing with any unsuitable material that is found in internet searches. This is highly unlikely due to the provision's filtering policy but any breach should be reported immediately to the centre manager or deputy.

### **Designated Safeguarding Leads:**

The Designated Safeguarding Leads (DSLs) should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

### **All Pupils:**

- Are expected to use the provisions ICT systems responsibly.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand the provision policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand the policy of the provision on the taking/use of images and cyber-bullying.
- Should understand the importance of adopting good e-safety practices when using digital technologies out of provision and realise that the

provisions E-Safety Policy covers their actions out of the provision, if related to their membership of the provision.

## **Parents / Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The provision will therefore take every available opportunity to help parents understand these issues through conversations and website information links.

## **Teaching and Learning**

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the provision has a duty to provide pupils with quality internet access as part of their learning experience:

- The provisions internet access will be designed expressly for pupil's use including appropriate content filtering.
- Pupils will, be taught discreet E-safety sessions during their first term with us.
- Pupils will be given clear objectives for internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the internet for research, including the skills of knowledge location, retrieval, and evaluation.
- As part of our P.H.S.E. & ICT curriculum, all year groups have digital literacy units that focus on different elements of staying safe online. These units include topics from how to use a search engine, our digital footprint and cyber-bullying.

## **World Wide Web**

The internet opens up new opportunities and is an essential part of the everyday world for children: learning, homework, and sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL, time and content shall be reported as soon as possible and a record of the incident made.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The provision will work with its technical support to ensure filtering systems are as effective as possible. SB Mentoring has in place web filtering that blocks access to most social media sites, chat rooms, online gaming sites and certain video hosting websites that do not have an internal filtering system.

## **E-mail**

E-mail is a quick and easy method of communication, and ensuring beneficial and appropriate usage is an important part of e-safety:

- Pupils may only use the google Google-issued e-mail platform.
- Pupils will only use the e-mail interface for curriculum purposes and the approved e-mail accounts set up on the provision's system for learning
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Should an email be sent to an external organisation then this should be done as a whole class, sent via the office and should be written carefully and authorised before sending, in the same way as a letter written on provision-headed paper.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

## **Social Networking**

Social networking Internet sites provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites in the provision is not allowed and will be blocked/filtered, wherever possible.

- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their provision or location. This will also include not using personal photographs and videos.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- All staff are advised not to have contact with parents and children on any social networking site.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the provision on social media and making any defamatory comments.
- For any queries, refer to the social media policy.

## **Mobile Phones**

Mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying or inappropriate contact.

- Pupils can bring mobile phones onto the provisions site only where it is seen by the provision and parents as a safety/ precaution use. (ie for the pupils arriving in taxis) These are handed to the duty mentor on arrival at 10am and collected at the end of the day at 2pm
- Staff should not use mobile phones to contact parents/guardians.  
Provision Staff will always use the provisions phone to contact parents/guardians.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff may only use their mobile phones for personal use in the staffroom before 10 am or after 2 pm.
- Staff are allowed to take digital/video images to support educational aims but must follow provision policies concerning the sharing, distribution and publication of those images. These images must be deleted within 24 hours.
- Care should be taken when taking digital/video images that pupils are dressed appropriately and are not participating in activities that put them at risk or bring the individuals or the provision into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission



- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- The manager or nominee will inform parents/carers and others present at provision events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.

### **SB Mentoring Website**

SB Mentoring's website is a valuable source of information for parents and potential parents.

- Contact details on the website will be the provisions address, email, and telephone numbers.
- Staff and pupils' personal information will not be made available.
- The manager will take overall editorial responsibility and ensure the content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the provisions website.

### **Information System Security**

- SB Mentoring's ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- E-safety will be discussed with all staff regularly.

### **Assessing Risks**

The provision will take all reasonable precautions to prevent access to inappropriate material. However, it is not possible to guarantee that unsuitable material will never appear on the provisions computers. The provision will audit ICT use to establish if

the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

## **Prevent Statement**

The counter-terrorism and security bill was granted royal assent on 21 February 2015, which places a statutory duty on named organisations, including educational establishments, to have due regard towards the need to prevent people being drawn into terrorism.

The most important part of this security bill is 'keeping pupils safe from the danger of radicalisation and extremism'.

The internet provides children and young people with access to a wide range of content, some of which is harmful. Extremists use the internet, including social media, to share their message. The filtering systems used at SB Mentoring and block inappropriate content, including extremist content. Where staff or pupils find unlocked extremist content they must report it to the Computing Co-ordinator or centre manager.

## **Cyber Bullying**

- Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils both in and outside provision. The methods and the audience are broader than traditional bullying and the perceived anonymity can make escalation and unintended involvement an increased risk. SB Mentoring have a range of strategies and policies to prevent online bullying, outlined in various sections of this Policy. These include:
- No access to mobile phones, public chat rooms, or Instant Messaging services on devices.
- Pupils are taught how to use the Internet safely and responsibly and are given access to guidance and support resources from a variety of sources. Specific education and training on cyberbullying (understanding what behaviour constitutes cyberbullying and its impact, how to handle concerns and report incidents) may be given as part of an annual Anti-Bullying Week and E-safety Events.
- Pupils are encouraged to discuss any concerns or worries they have about online bullying and harassment with their teachers.

- Pupils are informed on how to report cyberbullying both directly within the platform they are on, and to provision.
- Complaints of cyberbullying are dealt with in accordance with our Anti-bullying Policy.
- Complaints related to child protection are dealt with in accordance with our child protection procedures.

### **Handling e-safety complaints:**

1. Complaints of internal internet misuse will be dealt with by the centre manager.
2. Any complaint about staff misuse must be referred to the centre manager.
3. Complaints of a child protection nature must be dealt with in accordance with child protection procedures.
4. Pupils and parents will be informed of the complaints procedure.

## **Communication of Policy**

### **Staff and the e-safety policy:**

- All staff will be given the provisions e-safety policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

### **Parents and the E-safety Policy:**

- Parent's and schools attention will be drawn to the provisions e-safety policy on our website.
- They will receive regular updates on e-safety via leaflets and information sent via email.

## **Review**

This policy will be reviewed annually.

Louiza Bruce

Centre Manager