BIRMINGHAM INDEPENDENT COLLEGE

E-SAFTY POLICY

Created: January 2016

Reveiew: January 2018

1. Principle

1.1 With the increasing availability of devices, which give unrestricted access to the internet for children, Birmingham Independent College (BIC) considers online safety to be extremely important. We endeavour to ensure that every student in BIC's care is safe; and the same principles apply to the digital world as apply to the real world. This policy applies to all BIC staff, volunteers, visitors, parents and students.

1.2 IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. BIC has a responsibility to provide a safe environment in which children can learn. Our students are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, cyber-bullying, radicalisation, harassment, grooming, stalking and abuse.

2. Aims and objectives

2.1 The aim of this policy is to establish the ground rules we have in BIC for using ICT equipment and the Internet. New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school.

2.2 The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone but there are risks attached to them. Some of the dangers our pupils may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or 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.
- Extremism and radicalisation.
- Child Sexual Exploitation.

- 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.

2.3 Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically Anti-Bullying, Behaviour and Safeguarding & Child Protection.

2.4 As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' 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.

2.5 The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

3. Scope of the E-safety policy

3.1 BIC's E-safety policy is in line with the following national frameworks:

- Keeping children safe in education (July 2015)
- Ofsted Common Inspection Framework (September 2015)
- The Prevent duty (June 2015)
- Working together to safeguard children (March 2015)
- The Prevent Strategy (June 2011) and Channel guidance (April 2015)

3.2 This policy has links to the following policies:

- Safeguarding (including Child Protection)
- Behaviour
- Anti-bullying
- Data Protection

3.3 This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents/carers and visitors) who have access to and are users of school IT systems, both in and out of school. This policy, is implemented to protect the

interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

3.4 The Education and Inspections Act 2006 empowers Head of Colleges, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

3.5 The school will deal with such incidents within this policy and in associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

4. Roles & Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

4.1 Head of College

The Head of College is responsible for ensuring the safety (including e-safety) of all members of the school community, although the day to day responsibility for e-safety is delegated to all staff including Child Sexual Exploitation and extremism and radicalisation;

- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Adequate training is provided for staff in e-safety, including Child Sexual Exploitation and extremism and radicalisation;
- Effective recording and monitoring systems are set up and outcomes are rigorously analysed;
- Co-ordinating and reviewing an e-safety education programme in school;
- That relevant procedures in the event of an e-safety allegation are known and understood;
- Establishing and reviewing the school e-safety policies and documents;
- The school's Designated Child Protection Officers are trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

4.4 The Operations Manager

Is responsible for ensuring that:

- The school's ICT infrastructure is secure and meets e-safety technical requirements;
- The school's password policy is adhered to;
- The school's filtering and monitoring system is applied and updated on a regular basis;

- The use of the school's ICT infrastructure (network, e-mail, etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the Head of College for investigation/action/sanction.

4.5 Teaching & Support Staff
All teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- E-safety issues are embedded in all aspects of the curriculum and other school activities;
- Students understand and follow the school's e-safety policy and follow the guidelines on acceptable internet use in their planners;
- They monitor ICT activity in lessons, extracurricular and extended school activities;
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

4.6 Students

- Are responsible for using the school ICT systems in accordance with the guidance contained in their planners;
- All students are asked to sign an agreement pertaining to social media usage;
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials;
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy can also cover their actions out of school.

4.7 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues.

Parents and carers will be responsible for:

- Endorsing via signature this guidance pertaining to social media and social networking;

5. Education and Training

5.1 E-safety education will be provided in the following ways:

- E-Safety advice is provided as part of the form tutor and assembly programme and is regularly revisited lessons across the curriculum.
- Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Students are encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school during lessons.
- Students are taught about e-safety in the context of extremism and radicalisation and Child Sexual Exploitation.
- Rules for the use of ICT systems and the Internet are on noticeboards across BIC.
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

5.2 Staff Training

- The school will ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- E-Safety training will be provided to staff as part of their wider safeguarding responsibilities and will include a focus on Child Sexual Exploitation and extremism and radicalisation.
- All staff will participate in the Workshop Raising Awareness of Prevent (WRAP)
- All new staff receive the school E-Safety, Safeguarding and Child Protection Policies and Keeping Children Safe in Education (July 2015) and the school ensure that these documents are understood.
- Operations Manager will receive regular updates through the Local Authority and/or other information/training sessions and by reviewing guidance documents released.

6. The acceptable use of ICT, including social media

6.1 Email

- Digital communications with pupils (e.g. e-mail) should be on a professional level and only carried out using official school systems.
- Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses.
- School e-mail is not to be used for personal use.

6.2 Mobile Phones

- School mobile phones only should be used to contact parents/carers/students when on school business with students off site.
- Staff should not use personal mobile devices.
- Staff should not be using personal mobile phones in school during working hours when in contact with children.
- Students should adhere to the rules and guidelines set out in the Behaviour Policy regarding mobile phone use in school.

6.3 Social Networking Sites

Young people will not be allowed on social networking sites at school; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- Staff should not access social networking sites on school equipment in school or at home. Staff should access sites using personal equipment.
- Staff users should not reveal names of staff, pupils, parents/carers or any other member of the school community on any social networking site or blog.
- Students/Parents/carers should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders.
- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary.
- Students will be taught about e-safety on social networking sites as we accept some may use it outside of school. This will take place on Citizenship/PSHE days, during form time and within assemblies.

6.4 Digital Images

- The school record of parents who do not wish photos to be taken of their child is available from the Operations Manager.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Head of College.
- Where permission is granted the images should be transferred to school storage systems and deleted from privately owned equipment at the earliest opportunity.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use the internet in positive ways to publicise, inform and communicate information. The school has an active website which is used to inform, publicise school events and celebrate and share the achievement of students.

6.5 Websites

- In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Staff will preview any recommended sites before use. Certain websites are automatically blocked by the school's filtering system.
- "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger students who may misinterpret information.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff.

- All users must observe copyright of materials published on the Internet.
- Teachers will judge which students are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the students on the internet by the member of staff setting the task. All staff are aware that if they pass students working on the internet that they have a role in checking what is being viewed.
- Students should immediately report, to a member of staff the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Students must report any accidental access to materials of a violent, disturbing or sexual nature directly to a member of staff. Deliberate access to any inappropriate materials by a student will lead to the incident being dealt with under the school's Behaviour Policy. Students should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

6.6 Passwords

- Staff passwords or encryption keys should not be recorded on paper or in an unprotected file and should be changed at least every 3 months. Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems
- Students' passwords should not let staff know the passwords they use out of school. They must inform staff immediately if passwords are traced or forgotten so they can be reset.

6.7 Use of Own Equipment

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Head of College or the Operations Manager.
- Students should not bring in their own equipment unless asked to do so by a
- member of staff.

6.8 Use of School Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment;
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs.
- All staff should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

6.9 Data storage

- Staff are expected to save all data relating to their work to their Laptop if they have been assigned one
- The school discourages the use of removable media however if they are used we expect the Encryption of all removable media (USB pen drives, CDs, portable drives) taken outside school or sent by post or courier.
- Staff laptops should be encrypted if any data or passwords are stored on them.
- IEPs, assessment records, pupil medical information and any other data related to pupils or staff should not be stored on personal memory sticks but stored on an encrypted USB memory stick provided by school.
- Only take offsite information you are authorised to and only when it is necessary and required in order to fulfil your role. If you are unsure speak to a member of the Senior Leadership Team.

7. Monitoring and responding to incidents of e-safety

7.1 The Operations Manager will report any breaches, suspected or actual, of the school filtering systems to the Head of College. Any member of staff employed by the school who comes across an e-safety issue does not investigate any further but immediately reports it to the Operations Manager and impounds the equipment. (If the concern involves Operations Manager then the member of staff should report the issue to the Head of College).

7.2 Any e-safety incidents must immediately be reported to the Operations Manafer (if a member of staff) who will investigate further following e-safety and safeguarding policies and guidance.

7.3 It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. If any apparent or actual misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the Police will be contacted in the case of a pupil while the LADO will be contacted in the case of a member of staff to discuss a suitable course of action. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

8. Extremism and radicalisation

8.1 The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place and students are safe from radicalisation whilst online.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in lessons.

As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups and will receive annual training through in-school Safeguarding Training and the Workshop Raising Awareness of Prevent.

Appendix One

E-safety agreement

PARENTS

- There are a number of important steps you can take to ensure your children are safer when using sites such as Facebook, Twitter, Bebo, Snapchat, WhatsApp or KiK.
- Become familiar with the sites yourself.
- Encourage your children to keep their profiles private.
- Be careful about what information your children are sharing on the sites. DO you know all of your child's online friends?
- Encourage children to think about who they want to add as a friend.
- Make sure your children know where to go for help if they feel uncomfortable.
- If you don't want your children to access these services use parental control devices to block access to the sites.
- Remember that children must be 13 years or older to sign up for Facebook.
- Monitor the amount of time your child is spending on social networking sites.

PUPILS

- Be careful with personal information. As soon as information goes online you have lost control over who will see it and how it will be used. Don't post pictures that you wouldn't want everyone to see.
- Don't assume everyone you meet online is who they appear to be. The information provided by users when they register is not checked. Anyone can create a profile pretending to be someone else.
- Don't post information that could be used to find you in the real world.
- Don't reply to message that harass you or make you feel uncomfortable.
- Always explore the privacy settings of the site to protect your privacy and to protect yourself from strangers.
- Get your fiends and family to check your social networking site to check you are doing things safely.
- Keep your passwords to yourself.
- If you are the victim of cyber-bullying a) report the bully to the website b) keep evidence of what happened c) tell an adult
- Remember when you post something online you are posting it on the biggest screen in the world, which can be seen by billions of people.
- Please sign below to show that you have read the above advice.

Signed

Pupil: _____

Parent: _____

Head of College: _____

Date: _____

Appendix Two

Advice to students and staff

Our advice for parents

- There are a number of important steps you can take to ensure your children are safer when using sites such as WhatsApp, Kik, Facebook, MySpace or Bebo.
- Become familiar with the sites yourself
- Encourage your children to keep their profiles private.
- Be careful about what information your children are sharing on the sites.
- Do you know all of your child's online friends?
- Encourage children to think about who they want to add as a friend.
- Make sure your children know where to go for help if they feel uncomfortable.
- If you don't want your children to access these services use parental control devices to block access to the sites.
- Remember that children must be 13 yrs older to sign up for Facebook.
- Monitor the amount of time your child is spending on social networking sites.
- Riase any concerns you have regarding your child immediately to your child's Year Co-ordinator.

Our advice for pupils

- Be careful with personal information. As soon as information goes online you have lost control over who will see it and how it will be used.
- Don't post pictures that you wouldn't want everyone to see.
- Don't assume everyone you meet on-line is who they appear to be. The information provided by users when they register is not checked. Anyone can create a profile pretending to be someone else.
- Don't post information that could be used to find you in the real world.
- Don't reply to messages that harass you or make you feel uncomfortable.
- Always explore the privacy settings of the site to protect your privacy and to protect yourself from strangers.
- Get your friends and family to check your social networking site to check you are doing things safely.
- Keep your passwords to yourself.
- If you are the victim of cyber-bullying a) report the bully to the website, b) keep evidence of what happened and c) tell an adult.
- Remember when you post something on-line you are posting it on the biggest screen in the world, which can be seen by billions of people.
- For more information on E-Safety please visit, www.thinkuknow.co.uk/parents.