The Bosco Centre	
Policy:	**E-Safety Policy**
Applies to:	**College, Independent School, Nursery and Youth Clubs**
Reviewed:	**October 2018**
Next Review:	**October 2019**

The Bosco Centre expect all members of the centre (staff and students) to treat each other with care and respect. This is both in the real and virtual world. Our Safeguarding Policy describes the expected behaviours to keep all young people safe and free from abuse. This policy document expands on the practices described in that document to include all Information and Communication Technologies.

This policy applies to all members and users of The Bosco Centre, who have access to and are users of our ICT systems, both in and out of The Bosco Centre.

We will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a College computer or mobile device. The Bosco Centre College cannot accept liability for material accessed, or any consequences of Internet access.

Legislative Context

The Education and Inspections Act 2006 empowers the Principal to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, grooming, or other e-safety incidents covered by this policy, which may take place outside of the Bosco Centre College, but are linked to membership of the Bosco Centre College or youth clubs. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see attached). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The purpose of this policy is to:

- set out the key principles expected of all members of The Bosco Centre with respect to the use of ICT-based technologies.
- safeguard and protect the young people and staff of The Bosco Centre
- assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for The Bosco Centre

Content	exposure to inappropriate content, including online pornography, grooming and internet troll, ignoring age ratings in games (exposure to violence associated with often racist language extremism particularly towards 'radicalisation', substance abuse lifestyle websites, for example pro-anorexia/self-harm/suicide sites hate sites content validation: how to check authenticity and accuracy of online content
Contact	grooming/ sexual exploitation/ radicalisation cyber-bullying in all forms identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords
Conduct	privacy issues, including disclosure of personal information digital footprint and online reputation health and well-being (amount of time spent online (internet or gaming)) sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images) cf UKCCIS document 2016 copyright (little care or consideration for intellectual property and ownership – such as music and film)

Procedures

Our Principal or one of the Directors will act as first point of contact for reporting any incident.

Complaints of cyberbullying are dealt with in accordance with our Disciplinary Policy. Complaints related to child protection are dealt with in accordance with Safeguarding Policy and Southwark LEA child protection procedures.
When an incident occurs that involves one of the above risks student will be given information about infringements in use and possible consequences.

Consequences include (depending on the severity of the action):

- individual interviewed, followed by informing parents or carers;
- incident recorded under Causes of Concern with follow up
- counselling by mentors, safeguarding lead or Principal

- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- referral to Local children and young people's Safeguarding Board 0207 525 1921 and CEOP (child Exploitation and on-line protection 0870 000 3344)

We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

Acceptable use agreements

All students will be expected to sign an acceptable use agreement before they can access the college IT infrastructure. Acceptable use agreements to be held in student and personal files

Review and Monitoring

The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the Bosco Centre College.

Staff Training

We will ensure that all staff:

know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection
have access to regular training available to staff on e-safety issues. Staff training will be led by Alfredo Santos

as part of their induction process, all new staff with information and guidance on all aspects of safeguarding including e safety

Responsibilities of The Bosco Centre

Technology	**The Bosco Centre will:**
E-mail	Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account; Does not publish personal e-mail addresses of pupils or staff on the school website. Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law. Will ensure that email accounts are maintained and up to date Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police. Knows that spam, phishing and virus attachments can make e mails dangerous.
Website	The Principal will take overall responsibility to ensure that the website content is accurate and up to date. Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly

	the author's identity or status The point of contact on the web site is the Bosco Centre College's address and telephone number and we use a general email contact address, e.g. info@bosco.ac.uk. Home information or individual e-mail identities will not be published Photographs published on the web do not have full names attached; We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website

Responsibility of staff:

- No reference should be made in social media to students / pupils, parents / carers or Bosco Centre staff
- They do not engage in online discussion on personal matters relating to members of the College community
- Personal opinions should not be attributed to the Bosco Centre or the LEA
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Data Protection and Security

The Principal is the Senior Information Risk Officer (SIRO) and will deal with all occurrences of data protection breaches. We follow LEA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.

Equipment

Personal mobile phones and mobile devices

Mobile phones brought into the Bosco Centre College are entirely at the staff members, students, parents or visitors own risk. The B.C.C. accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

Student mobile phones which are brought into school must be handed in to a member of staff at the beginning of each lesson. Students may use their phones during school break times.
All visitors are requested to keep their phones on silent.

The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Principal / parents. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Principal is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

The B.C.C. reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring. (CC Education Act 2011)

Where parents or students need to contact each other during the college day, they should do so only through the B.C.C.'s telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.

Students' use of personal devices

If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences

Staff use of personal devices

Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.

Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Staff will use the Bosco Centre phone where contact with students, parents or carers is required.

Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.

Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

If a member of staff breaches the Bosco Centre's policy then disciplinary action may be taken.

Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then the College 'phone will be provided and used. In an emergency where a staff member doesn't have access to the College 'phone, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video

We gain parental / carer permission for use of digital photographs or videos involving their child as part of the B.C.C, agreement form when their daughter / son joins the College (Years 10 and 11)

We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;

Staff sign the College's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;

If specific pupil photos (not group photos) are used on the College web site, in the prospectus or in other high profile publications the school will obtain individual parental or student permission for its long term use where applicable.

Students are taught about how images can be manipulated in their e Safety education programme.

Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or college. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Darren Coghlan CEO and Principal		**Review date**	**October 2018**
Prim Campbell Chair of Trustees		**Next Review**	**October 2019**

Appendix 1: Roles and Responsibilities

Role	Key Responsibilities
Principal	• To take overall responsibility, having delegated persons for: • e-Safety provision • responsibility for data and data security. (SIRO) • use of an approved, filtered Internet Service, which complies with current statutory requirements • ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • awareness of procedures to be followed in the event of a serious e-Safety incident. • regularly monitoring e-safety procedures at the Centre • ensuring that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager) • facilitating training and advice for all staff • ensuring that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • ensuring appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • keeping up-to-date documentation of the B.C's e-security and technical procedures – ICT Co-ordinator
Designated Child Protection Lead	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that e-safety education is embedded across the curriculum • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident • To ensure that an e-Safety incident log is kept up to date • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: o sharing of personal data o access to illegal / inappropriate materials o inappropriate on-line contact with adults / strangers o potential or actual incidents of grooming o cyber-bullying and use of social media • Each project area has designated CPL
Admin Officers	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place

Role	Key Responsibilities
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
Students	• Read, understand, sign and adhere to the Student Acceptable Use Policy • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • to know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To 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 covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home • to help the school in the creation/ review of e-safety policies
Parents / carers	• to support the school in promoting e-safety • to read, understand and promote the school Student Acceptable Use Agreement with their children (Years 10 and 11). • to consult with the school if they have any concerns about their children's use of technology

Appendix 2: Pupil e-Safety curriculum

The Bosco centre College has a clear, progressive e-safety education programme as part of the ICT curriculum / Personal Development curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- To understand why and how some people will 'groom' young people for sexual reasons;
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying, grooming, extremism
- To know how to report any abuse including cyberbullying; and how to to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.
- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through the Acceptable Use Policy which every student will sign/will be displayed throughout the B.C.C.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;

- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling.