



# BRADFIELD COLLEGE

## E-Safety Policy

<b>Document Control</b>	
Document title:	E-Safety
Author:	Sarah Davies, Deputy Head (Pastoral)
Document status:	Approved
Approved by:	Pastoral Committee
Effective Date:	September 2019
Version number:	2.0
Date of next full review:	September 2020

<b>Version</b>	<b>Author</b>	<b>Date</b>	<b>Changes</b>
1.0	T Benstock	Feb 2018	Update on IT security
2.0	S Davies	Sept 2019	Reviewed



BRADFIELD COLLEGE

# E-Safety Policy

*Reviewed February 2018*

# Contents

1. STATEMENT OF PRINCIPLES .....	5
2. POLICY REACH .....	5
3. WHAT IS E-SAFETY? .....	5
4. E-SAFETY RESPONSIBILITIES AT BRADFIELD COLLEGE (CF ANTI-BULLYING POLICY APPENDIX B3) .....	6
4.1 <i>All Staff</i> .....	6
4.2 <i>All Pupils</i> .....	6
4.3 <i>E-Safety Committee</i> .....	6
4.4 <i>Pupil E-Safety Committee</i> .....	6
4.5 <i>Director of IT Services</i> .....	6
4.6 <i>Wellbeing and E-Safety on the Curriculum</i> .....	7
4.7 <i>DSL and Deputy DSL</i> .....	7
5. THE COLLEGE RESPONSE TO BREACHES OF E-SAFETY (CF ANTI-BULLYING POLICY APPENDIX B3) .....	7

# E-Safety Policy

Last reviewed: February 2018

## Safeguarding Mission Statement

Bradfield College is committed to providing a caring, friendly and safe environment for all its pupils so they can learn in a relaxed and secure atmosphere. The College takes seriously its responsibility to protect and safeguard its pupils. Ours is a TALKING school. This means that anyone who has worries about a pupil in the College ought to talk about it. Telling is not “dobbing in” or “grassing”.

## 1. STATEMENT OF PRINCIPLES

This policy aims to ensure that all pupils and staff at Bradfield College use technology in such a way as to protect and promote the welfare of all members of the community, and of the pupils in particular. The whole ethos of Bradfield College aims to create amongst all who work or study here mutual respect and understanding of the needs of others.

This policy will be made available to staff, pupils and parents via the Bradfield Website, the College Intranet (Firefly) and in hard copy from the Second Master’s office. Because of the rapidity of on-going developments in young people’s on-line experience, this E-Safety policy is kept under on-going review. The next full review is due to be completed (and ratified by the College Pastoral Committee) at the 2018 Lent Half Term break.

## 2. POLICY REACH

The policy for E-Safety applies to all pupils, College employees, volunteers working at the College, and to agents employed indirectly by the College. It also applies to members of Council, the College governing body. It is designed to sit alongside, and should be read in conjunction with, other related College policies such as the Child Protection and Safeguarding Policy, the Anti-Bullying Policy, the Behaviour Policy, the Acceptable Use Policy, and the Social Media Policy.

## 3. WHAT IS E-SAFETY?

Whilst the Internet and associated technologies are excellent tools and resources to enrich learning, there are still dangers related to their use. Some examples of these might include:

- Cyberbullying – typically, malicious messages or images sent via email, forums or SMS (cf Anti-Bullying Policy Sections 3.7-3.8)
- Potential exposure to inappropriate and/or adult material
- Illegal behaviour – including hacking, spamming or viewing/downloading pirated media/games
- Obsessive internet use – typically through social media, forums or gaming sites
- Potential exposure to sexual predators posing as peers
- Downloading malware, viruses, Trojans, trackers/loggers that are packaged anonymously within software, apps or web pop-ups
- Using proxy or VPN services to purposely bypass the filtering services
- Fake account creation – on any platform that purports affiliation or interacts with the College is not permitted
- Sharing of password or private account details is not permitted. If a password or breach is suspected please report this to IT Services immediately and change all associated passwords

Bradfield College will assume responsibility for protecting all members of our community from such dangers.

#### **4. E-SAFETY RESPONSIBILITIES AT BRADFIELD COLLEGE (CF ANTI-BULLYING POLICY APPENDIX B3)**

---

##### **4.1 All Staff**

E-Safety will be the concern of all staff at the College. All adults acting *in loco parentis* and who come into contact with children have a 'duty of care' for them, and this duty of care extends to all matters relating to the use of technology. All staff who work at Bradfield College will receive regular training in their child protection responsibilities, and all teaching staff will receive specific training in matters of E-Safety, including use of the internet and cyberbullying. In particular, all staff will have a clear understanding of E-Safety issues, know how to report E-Safety concerns, abide by the staff AUP (Acceptable Use Policy), give due concern to the reputation of the College and its members before they post online, contribute to a whistleblowing culture where they have any suspicion or concern, and never befriend current pupils on social media themselves.

##### **4.2 All Pupils**

All pupils at the College will contribute to the ethos of the College by showing respect for and understanding of the needs of others. In addition they will comply with the AUP (Acceptable Use Policy) each time they login to the Bradfield network. Furthermore, they will participate in and gain an understanding of E-Safety matters from ELW provision, assemblies, lectures and informally in houses. Ours is a talking school, and pupils will report any concerns they may have regarding E-Safety issues. All pupils will know how to report E-Safety concerns via Firefly, or by telling a trusted member of the College Staff.

##### **4.3 E-Safety Committee**

The E-Safety Committee, reporting to the Pastoral Committee, will provide a consultative group with wide representation from the school community. It will have oversight of issues regarding E-Safety (including the College's education of pupils, staff and parents), and responsibility for monitoring policy in the light of emerging technologies.

##### **4.4 Pupil E-Safety Committee**

The Pupil E-Safety Committee will report to the E-Safety Committee. It will be made up of interested pupils from across the spectrum of the pupil body. Its purpose will include the regular review of current trends in technology, advising the E-Safety Committee on pupil use of new technologies, and informing E-Safety College.

##### **4.5 Director of IT Services**

The Director of IT Services will have overall responsibility for ensuring the best technological solutions are in place to ensure E-Safety (to include filtering and monitoring software), whilst still enabling the pupils to use the Internet effectively in their learning. They will also ensure that all information captured using these systems is securely stored, and accessible to appropriate members of staff. They will perform regular audits of the College network to ensure that no inappropriate data is stored or accessible via local storage, they will assist with the development

of the E-Safety education programme for pupils and staff, and they will sit on the E-Safety Committee to help advise on E-Safety matters and review E-Safety policy.

#### **4.6 Wellbeing and E-Safety on the Curriculum**

The Head of Wellbeing will be responsible for delivering E-Safety instruction on the curriculum and for the Wellbeing lecture programme that includes talks on E-Safety related matters. They will also sit on the E-Safety Committee.

#### **4.7 DSL and Deputy DSL**

The DSL (Designated Safeguarding Lead) will have an operational duty to act as the lead person in matters of Child Protection and Safeguarding. He or she will also maintain the College Bullying Register, which records all instances of Cyber-bullying.

The Deputy DSLs will work with the DSL to ensure that policies, protocols and records regarding Child Protection and Safeguarding are up-to-date. Full details of their roles can be found in the Child Protection and Safeguarding Policy.

### **5. THE COLLEGE RESPONSE TO BREACHES OF E-SAFETY (CF ANTI-BULLYING POLICY APPENDIX B3)**

---

Bradfield College will use its existing procedures to deal firmly, fairly and decisively with any examples of inappropriate ICT use, complaints or allegations, whether by an adult or a pupil. (These may include breaches of filtering or the AUP, illegal use, cyberbullying, or the use of ICT to groom a child or to perpetrate abuse.)

The College is determined to combat cyber-bullying and recognises that the effects of online bullying can often be amplified by the potential reach of material posted online, the greater scope for bringing the College into disrepute, and the additional anxieties that can be caused by the abuse of online anonymity. Pupils will additionally be held responsible for material they have posted when absent from the College premises. Sanctions can include the confiscation of mobile phones or personal computers, gating, suspension and expulsion.