E-Safety Policy and
Agreed Acceptable use of ICT

We believe that ICT has a critical role in equipping students for life in the 21st century and that ICT can have a positive impact on teaching and learning. To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom. This policy document has been drawn up to protect all parties – the students, the staff and the school, and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Staff Responsibilities

All staff are responsible for promoting and supporting safe behaviour in their classrooms and for following e-safety procedures. Staff should also be aware of their personal responsibilities to protect the security and confidentiality of the school network.

To comply with for Data Protection:

- If you have a school telephone it must be password protected
- Unless you have a school telephone you should not download 365 on to your device.
- If you do have a school telephone you should only use your emails on it. Do not open other applications from 365 on it.
- If you are working on 365 from your home, you must work in the cloud- never save information on your school iPad or laptop.
- You must login and out every time you use 365.
- You must log out of 365 before you leave school.

WhatsApp

- Never use WhatsApp to talk about pupils or parents (it is not secure)
- Never create a WhatsApp group with parents unless you have their individual consent to do so.

- Never create a WhatsApp group with parents unless you have their individual consent to do so.

To Safeguard the Children

The Green paper, 'Every child matters' together with the provisions of the Children's Act 2004, the policy document Working Together to Safeguard Children, Keeping Children Safe in Education 2018 and Working Together to Keep Children Safe 2018 set out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes the aims that children and young people are:

- Safe from maltreatment, neglect, violence and sexual exploitation
- Safe from accidental injury and death
- Safe from bullying and discrimination
- Safe from crime and antisocial behaviour in and out of school
- Secure, stable and cared for.

These aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, there is a need to protect pupils from dangers such as:

- The use of the internet for grooming children and young people with the ultimate aim of exploiting them sexually.
- The use of ICT as a new weapon for bullies, who may torment their victims via websites, text messages or exposure to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of all staff 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 school's physical buildings.

In addition and in order to make our students aware of these dangers PSHEE lessons will include the teaching of online activities such as grooming and sexting and the discussion of cyber bullying, its characteristics, effects on the victims and the sanctions by the school. In KS4 and 6th Form, training sessions will be arranged to alert students to these forms of abuse and the BST zero tolerance of same.

At BST we know that children with special educational needs (SEND) or disabilities are particularly vulnerable to online abuse and for this reason we strive to make sure every member of staff works to help these children feel part of the school community and thus

increase their resilience to any form of abuse.

Members of the police force are invited to the school to give further training on Online Safety to children in Year 7, under the local online safety provision for school children on the island.

As radicalization and extremism is also conducted online, all members of staff will attend a training course on this topic given by the National Police.

Along with these steps to help safeguard children, the school has in place a web filtering system to prevent students from viewing inappropriate content.

At BST all our students know that they can approach any member of staff if they have a problem and that they will be listened to and their concern be taken seriously.

Parents are also provided with information about online abuse including what actions the school takes to prevent it and support those children affected by it.

To Ensure Security and Confidentiality

- All students must maintain password security on the network. Passwords should not be shared with any other member of the school's community, nor should they be written down. Class Teachers will keep a class list of pupil's passwords and usernames.
- Staff laptops must also be password protected, as teachers are responsible for any inappropriate material found on their laptops or computers.
- All computers and associated equipment must be shut down and turned off at the end of the day.
- Data storage devices such as USB pens, portable hard drives, CD ROMs and DVD ROMs must be subject to virus protection measures by 'stopping' devices before removal from the computer, and not inserted in the first instance if the source cannot be trusted. USB pens should be cleaned before 0 used in school computers or laptops. As a preventative measure, KS3 USB pens should not be taken out of school at any time.
- Teachers should monitor student iPads when in use in their lessons
- Any accidental access of inappropriate material on the internet should be reported to the head teacher immediately. The school reserves the right to examine internet access logs from any computer in the school and staff laptops issued by the school. The school cannot accept liability for material accessed, or any consequences of Internet access.
- Software should not be downloaded unless the source can be trusted and the member of staff has checked that there is no infringement of licensing laws.
- Photographs of students should only be taken and saved on the network where permission to do so has granted by parents.

- Take care to investigate websites personally before directing the children to use them.

To Safeguard the Facilities and Support Student Behaviour

- Students must always be supervised in ICT suites and in classrooms where laptops/computers/iPads are in use.
- Upon discovery, all damage must be reported immediately.
- Ceiling projectors must be turned off when they are not in use by using the remote control.
- Food and drink must not be consumed in ICT suites or in classrooms where laptops are in use.

How will complaints regarding E-Safety be handled?

The school 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 school computer or mobile device.

Sanctions available for misuse of computers and iPads are:

- Interview, counselling and/or disciplinary action by the teacher, ICT Co-ordinator or Head teacher
- Informing parents or carers
- Removal of internet or computer access for a period, (which could ultimately prevent access to files held on the system).
- Referral to Police or Social Services.

The Designated Safeguarding Lead will act as first point of contact for any complaint. Any complaint about staff misuse will be referred to the Head teacher and may result in formal disciplinary proceedings.
Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.