PLATANOS COLLEGE

Statement of Intent

We are committed to providing a caring, friendly and safe environment for all of our pupils so that they can learn in a relaxed and secure atmosphere. We believe every pupil should be able to participate in all school activities in an enjoyable and safe environment and be protected from harm. This is the responsibility of every adult employed by, or invited to deliver services at, Platanos College. We recognise our responsibility to safeguard and promote the welfare of all our pupils by protecting them from physical, sexual or emotional abuse, neglect and bullying.

E-SAFETY POLICY AND CODE OF PRACTICE

2015 – 2016

This Policy should be read in conjunction with the Safeguarding Policy

E-Safety Policy and Code of Practice

Principles

The School's E-Safety Policy reflects the importance it places on the safe use of information systems and electronic communications. This Policy concerns safeguarding children and young people in the digital world.

E-Safety encompasses internet technologies (including social networking sites) and also electronic communications via other means such as mobile phones, tablets, games consoles and wireless technology.

The School's ICT systems and equipment are intended to promote effective communication and learning. However, the School recognises that it has a responsibility for ensuring that its pupils are protected from contact with inappropriate material.

E-Safety also emphasises learning to understand and use new technologies in a positive way and to develop safer online behaviours both in and out of school.

All users should understand that network activity and online communications made via the School network are monitored. The School operates a rigorous network filtering system to prevent its pupils from exposure to inappropriate material.

Scope

This Policy applies to all members of the School. This includes (but not exclusive to) staff, pupils, parents/carers, volunteers and visitors who have access to and are users of the School's ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, 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 action for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered, which may take place out of school, but is linked to membership of the school.

The School will deal with such incidents within this Policy and the associated Discipline and 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.

Responsibilities

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the Policy. This will be carried out by the Governors receiving regular information about e-safety or a designated *E-Safety Governor*.

- Regular meetings regarding e-safety.
- Regular monitoring of e-safety incidents.

Headteacher and Senior Leaders

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the *E-Safety Co-ordinator / Officer*.
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator / Officer.
- The Headteacher and another member of the Senior Management Team 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.

E-Safety Coordinator / Officer

- leads the e-safety committee and liaises with the Designated Senior Person for Child Protection.
- takes day to day responsibility for e-safety issues and plays a role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides/co-ordinates training and advice for staff and pupils
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with Headteacher / relevant Governor(s) to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings / committee of Governors
- reports regularly to Senior Management Team

Network Manager / Technical staff

The Network Manager / Systems Manager / ICT Technician / ICT Co-ordinator is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets e-safety technical requirements
- that users may only access the school's networks through properly enforced password protection
- the school's filtering and monitoring systems is applied rigorously and updated on a regular basis
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Officer /Headteacher / Senior Leader or relevant member of staff

All Other Staff

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
- they have read, understood and signed the Electronic Communications Acceptable Use Policy / Agreement
- they report any suspected misuse or problem to the E-Safety Co-ordinator / Officer /Headteacher / Senior Leader or relevant member of staff for investigation / action.
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students / pupils understand and follow the school e-safety and acceptable use policy
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students / 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

Volunteers and Other Users

Must familiarise themselves with this Policy and sign and abide by the Electronic Communications Acceptable Use Policy.

Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and electronic communication 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 every opportunity to help parents/carers understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the E-Safety Code of Practice (below)
- accessing the school website, VLE and similar services in accordance with the Electronic Communications Acceptable Use Policy

Pupils

In order to ensure a safe learning environment, all pupils are required to agree to abide by the following rules which form the School's E-Safety Code of Practice:

- I will follow the School's systems and guidance on the use of mobile phones and other digital technology and on reporting abuse, misuse or access to inappropriate materials.

- I will only use the School's ICT systems, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.

- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not take images of pupils, staff or any other child/young person. I will not download or distribute any images of pupils, staff or any other child/young person using phones, computers, social networking sites or any other methods. Such activity can cause offence and is a form of cyber-bullying.
- I will not access social networking sites and similar sites using school ICT systems.
- I will not download or install software on School technologies.
- I will only log on to the School network/ Learning Platform with my own user name and password.
- I will follow the School's ICT security system and not reveal my passwords to anyone and will change them regularly.
- I will only use my school e-mail address at school.
- I will make sure that all ICT communications with pupils, teachers or others are responsible and sensible.
- I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone that I have met through the internet.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils, my family or others any distress or bring any of them into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times and I will not interfere with or delete any other pupil's work.
- I will not copy any work belonging to another pupil or from the internet and pretend that it is my own work.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

E-Safety Policy and Code of Practice Agreement

Parent(s)/carer(s) and pupil

ICT (information and communications technology) including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our School. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of E-Safety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss the E-Safety Policy and Code of Practice with their parent(s) or carer(s) and then sign and follow the terms of the agreement. Any questions or concerns can be discussed with their form tutor or ICT teacher.

Please sign and return this agreement to the School.

Signatures

We have discussed this document and ……..……...……..... (pupil's name) agrees to follow the E-Safety rules to support the safe and responsible use of ICT at Platanos College.

Parent/Carer's signature: ……..……...…….

Pupil's signature: ……..……..…….

Tutor group: ……..……...…. Date: ……