

#### **Introduction:**

The rapid growth of the internet and of electronic technologies has opened a world of exciting opportunities for students. New technologies have become integral to the lives of students today, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Students always have an entitlement to safe internet access.

This e-safety policy is designed to help to ensure safe and appropriate use. The use of these new technologies can put students at risk within and outside the school. Through the internet and mobile technology, it is possible for students to have access to almost unlimited information worldwide, to be entertained with films and music and, through social networking sites, to contact and socialize with other young people. However, alongside the benefits there are also risks and, while many young people are very competent in using these technologies, their knowledge and understanding of the risks is often very low.

E-safety refers to child protection and safeguarding of both children and adults in the digital world. It is about learning to understand and use technologies in a safe, positive way. It is also about supporting students and adults to develop safe online behaviours (both in and out of school).

E-safety is largely concerned with internet communications. The internet is accessible from computers, laptops, tablets, mobile 'phones, games consoles and other devices like the iPod Touch and internet connected TV. Other communication technologies, such as texting and 'phone calls, are also covered by the term 'e-safety'

The risks to students are various:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / 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
- 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.

Many of these risks reflect situations in the off-line world and as such this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies). 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.

Students need to be protected from these risks and they need to be helped to develop the skills to keep themselves safe when they are online.

---

**Four Cs that may present risks to students using technologies:**

- **Content:** students may be exposed to inappropriate content which may upset or embarrass them, or which could potentially lead to their involvement in crime and anti-social behaviour.
- **Contact:** some people use the internet to groom children with the ultimate aim of exploiting them sexually. ICT offers new weapons for bullies who may torment their victims, for instance using websites or text messages. Social networking sites bring e-safety challenges, with many young people making available online some detailed – and sometimes inappropriate – personal information, which again raises both content and contact issues.
- **Commerce:** while the internet offers new opportunities for doing business online, it also brings with it many unscrupulous traders to whom children and young people may be particularly vulnerable.
- **Culture:** bullying via websites, mobile phones and other forms of communication device. Downloading of copyrighted materials e.g. music and films.

**Scope of the Policy**

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. The school will deal with e-safety incidents in the same way as associated behaviour and bullying incident and will, where it becomes aware, inform parents / carers of incidents of inappropriate e-safety behaviour that take place outside of school.

The e-safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Should serious e-safety incidents take place, the following external persons / agencies should be informed as appropriate.

**Implementation:** It is the responsibility of line managers to ensure that staff members are aware of and understand this policy and any subsequent revisions.

The head teacher is responsible for ensuring the safety (including e-safety) of all members of the school community, though the day to day responsibility for e-safety can be delegated.

**Infrastructure:**

Access to the internet needs to be through equipment and connections that will allow for a good level of protection, filtering, and adult control.

**Location of Internet Access**

Internet access points at Dibden Park School are sited in communal areas that allow for reasonable oversight and monitoring of young people's use.

**Security Software**

Dibden Park school reviews the security software currently available and ensure that suitable security is installed to reduce the risk of virus, Trojans, adware and cookies.

**Age Related Filtering and Blocking**

Dibden Park school has a filtering and blocking criteria and determines which sites they will block and which sites will be allowed to be viewed by certain age groups.

---

### **Spam Filtering and Blocking**

Dibden Park School uses effective filtering / blocking systems.

### **Curriculum:**

E-safety is a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum:

- In lessons where internet use is pre-planned, it is best practice that 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.
- Where students are allowed to search the internet independently in lessons, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that ICT support can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

### **Teaching Internet Safety:**

The teaching of e-safety is embedded throughout the curriculum across the age ranges of the School. Students study a program of PSHE from KS2-KS4 and e-safety sessions are planned within those schemes.

Sessions are delivered through the weekly PSHE lessons and they are planned based on the requirements and needs of the year groups. These sessions are complemented by tutors and special events such as safer internet days.

Through teaching ICT Dibden Park School equips students to participate in a rapidly changing world where work and leisure activities are increasingly transformed by technology. We enable them to find, explore, analyse, exchange and present information in a varied and stimulating way. ICT skills are a major factor in enabling them to be confident, creative and independent learners. As the aims of ICT are to equip students with the skills necessary to use technology to become independent learners, the teaching style that we adopt is as active and practical as possible. We provide suitable learning opportunities for all pupils by matching the challenge of the task to the ability and experience of the student. ICT helps students learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The e-safety policy encourages appropriate and safe conduct and behaviour when achieving this.

### **Training for Staff:**

All staff will be provided with access to information and training resources about e-safety. This will include understanding how e-safety relates to other company policies such as safeguarding and bullying.

### **Supervision and Monitoring:**

Dibden Park School will monitor the effectiveness of e- safety measures and will alter and update them as changes emerge on the internet.

Dibden Park School will keep the effectiveness of its e-safety measures under review to ensure they remain 'fit for purpose'.

### **Working with students about Internet Safety at Dibden Park School**

- Help students to understand that they should never give out personal details to online friends they do not know offline.
- Explain to students' what information about them is personal: i.e. email address, mobile number, school name, sports club, arrangements for meeting up with friends and any pictures or videos of themselves, their family or friends. Small pieces of information can easily be pieced together to form a comprehensive insight into their lives and daily activities.
- Ensure students are aware that they need to think carefully about the information and pictures they post on their profiles. Inform them that once published online, anyone can change or share these images of them. Advise them not to post any pictures, videos or information on their profiles, or in chat rooms, that they would not want a parent or carer to see.
- Remind students who receive spam or junk email and texts, that they should never open them, or if they do, do not believe their contents, never reply to them or use them.
- Ensure that students understand that some people lie online and that therefore it's better to keep online mates online. They should never meet up with any strangers without an adult they trust.
- Always keep communication open for a child to know that it's never too late to tell someone if something makes them feel uncomfortable.

In the event of breaches in internet safety Dibden Park School will ensure that learning takes place to prevent a reoccurrence. Issues will be shared across the company to support opportunities for wider learning and the dissemination of best practice.