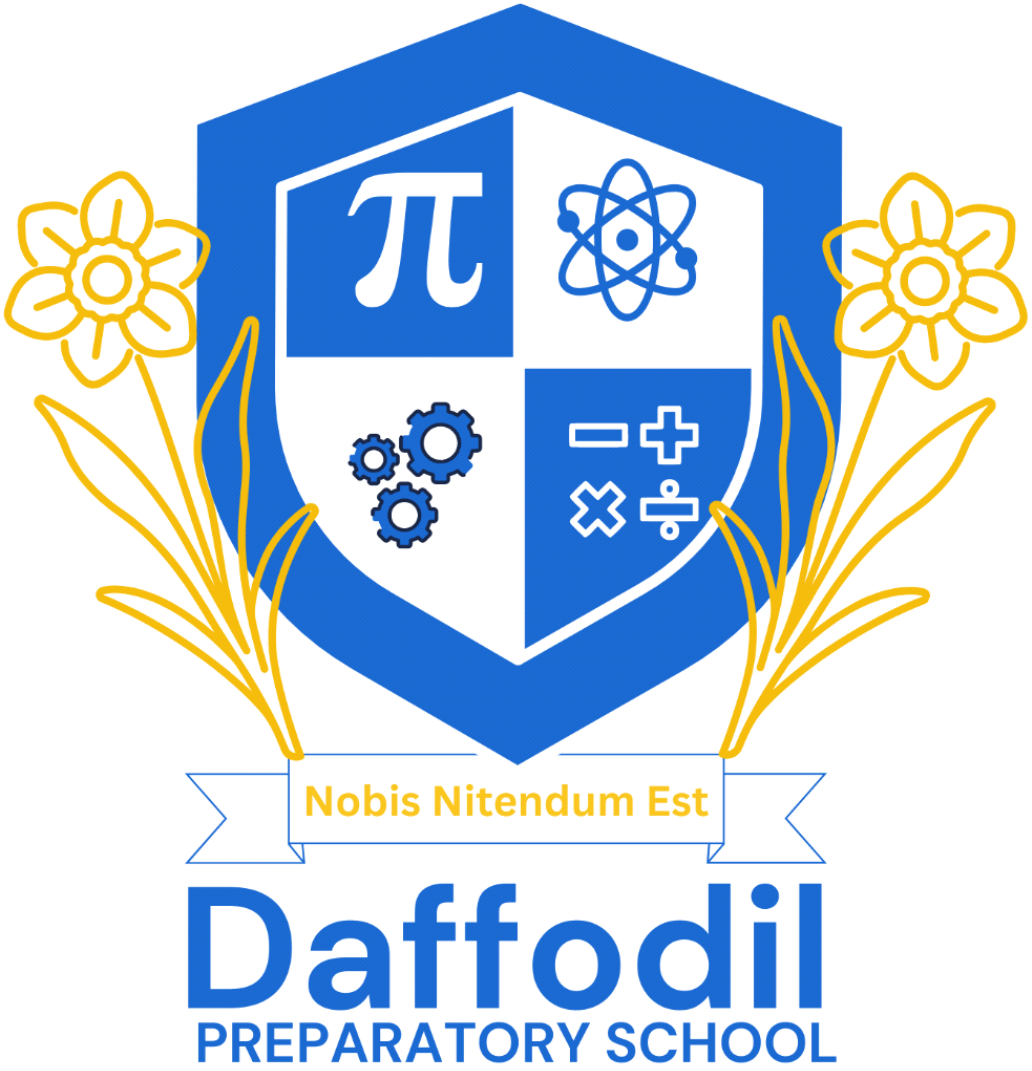

E-Safety Policy

Last reviewed: August 2025

Date of Next Review: August 2026

Reviewed by: Governing Body

Version 1.2

1 TABLE OF CONTENTS

At Daffodil Preparatory School, we believe that every child should be given the opportunity to develop to the highest standard academically, with good morals, social skills and cultural awareness to become a well-rounded individual. Through our Vision, Ethos and Aims, at Daffodil Preparatory School we provide this opportunity for our children and are pleased to do so within our school environment.

We anticipate all applicants to give their commitment, respect and wholehearted support to uphold and maintain our school ethos and values. In line with our values, we do not tolerate extreme religious or political views in any capacity. This includes any views which are prohibited under the law as well as those views that contravene our ethos and stance or equality, tolerance and respect for all, regardless of race, gender, faith (or none) or sexual orientation or gender preference.

2 AVAILABILITY OF THE POLICY (REG 33(B))

This policy is available to all parents and carers:

- On the school website: www.daffodilprepschool.org.uk
- In printed form upon request from the school office

3 INTRODUCTION

At Daffodil Preparatory School, we are committed to keeping every pupil safe and healthy, both in the physical and digital world. The E-Safety Policy operates under the umbrella of the **Safeguarding Policy**, ensuring that the same 'staying safe' outcome outlined in the *Every Child Matters* agenda applies equally to the online and electronic environment.

We recognise that the internet plays a vital role in a child's education. Used responsibly, it enriches and extends learning, supports pupil achievement, and raises educational standards. It also assists staff in their teaching and contributes to the effective management of the school.

Our approach to e-safety is guided by the **Independent School Standards Regulations (ISSRs)** and meets the expectations of **Ofsted**, which require schools to demonstrate robust safeguarding, a safe online environment, and the active promotion of **British Values**, including respect, responsibility, and the protection of pupils from risks such as online abuse, extremism, or exploitation.

4 AIM

The purpose of the e-safety policy is to maximise the educational benefit and fulfil the obligation of providing quality internet access to students as part of their lifelong learning experience, whilst adopting a safe culture and minimising any associated risks.

Students shall be educated about the benefits and the risks of using technology and controlling their online experience.

5 INTERNET ACCESS

- The use of internet is a part of the statutory curriculum and an essential tool for staff and students.
- The use of internet enhances learning opportunities.
- The internet is used and integrated into the planning to enrich and extend learning activities.
- The internet shall benefit education by allowing access to various educational resources.

6 MANAGING INTERNET ACCESS

- Internet access is designed particularly for pupils' use reflecting the curriculum requirements and includes filtering appropriate to the age of students.
- Students are given clear objectives for Internet use and are taught what Internet use is acceptable and what is not.
- Students are taught how to evaluate Internet content.
- Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students are taught to cross-check information and validate information before accepting its accuracy.
- Students are taught how to report unpleasant Internet content or if unsuitable sites are discovered.

7 INTERNET ACCESS SECURITY

- The security and capacity of the school information systems is reviewed regularly.
- Virus protection is installed and updated regularly.

8 MANAGING E-MAIL

- Pupils and staff shall only use approved e-mail accounts on the school system.
- Personal e-mail or messaging between staff, parents and pupils shall not take place.
- Personal details of themselves or others shall not be revealed in e-mail communication, or an arrangement to meet anyone without specific permission.

- On occasions an e-mail shall be authorised before sending to an external organisation just as a letter written on school headed notepaper would be.
- The forwarding of chain letters is not permitted.

9 MANAGING WEB SITE CONTENT

- The point of contact on the school web site shall be the school address, e-mail and telephone number.
- Staff or students' personal information is not published.
- The Governing Body has overall editorial responsibility and ensures that content is accurate and appropriate.
- The school's ethos is reflected in our website, ensuring that information is accurate, well-presented and personal security is not compromised.
- Care is taken to ensure that all information is considered from a security viewpoint including the use of photographic material.
- Photographs of pupils are not used without the written consent of the pupil's parents/carers.
- Use of site photographs is carefully selected so that any pupils cannot be identified, or their image misused.
- The names of pupils are not used on the website, particularly in association with any photographs.
- The copyright of all material on the website will be held by the school.

10 SOCIAL NETWORKING AND CHAT ROOMS

- The school blocks/filters access to social networking sites
- Newsgroups are blocked unless a specific use is approved by the Head teacher.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. I.e. Real name, address, mobile or landline phone numbers, school, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for pupils.
- Pupils are taught the importance of personal safety when using social networking sites and chat rooms.
- Pupils are not allowed to access public or unregulated chat rooms.
- Staff shall not exchange social networking addresses or use social networking sites, under any circumstances, to communicate with pupils.

- Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil is necessary, the agreement of a member of SLT shall always be sought first and language used shall always be appropriate and professional.

11 MANAGING FILTERING

- The school works in partnership with parents/carers; the Local Authority, the DCFS and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.
- Filtering methods are selected by the school in consultation with its IT partner and with the LA to ensure that they are age and curriculum appropriate.
- Regular checks by Senior Staff are undertaken to ensure that the filtering methods selected are appropriate, effective and reasonable.
- If staff or pupils discover unsuitable sites, the URL and content shall be reported to SLT immediately.

12 POTENTIAL RISKS

Internet and electronic communications technologies derive huge educational benefits but also carry potential risks. Some of the potential risks are highlighted below:

13 CONTENT

- Students shall be protected from viewing and/or downloading adult material, violence, racist/hate sites, potential grooming and extremist material.
- Students are made aware of the potential long-term effects of any inappropriate content that they upload themselves, such as photographs, too much personal information or nasty comments about others.
- Students are educated about the need to understand that anyone can publish anything they wish on the Internet, so it may be inaccurate.
- In addition, students are educated about the need to understand inappropriate use of the Internet and respecting copyright issues.

14 CONTACT

There are people who will try their utmost to gain access to students to do them harm. The dangers of contact with persons unknown are made clear.

15 COMMUNICATION

- Students shall be protected and made aware of the potential dangers of digital communication (i.e. you can never be 100% sure that you know who you are communicating with!).
- Safe use/potential dangers of email use, instant messaging, chat rooms, social networking sites etc. are explored and made clear to pupils.
- The dangers of using digital imaging devices such as cameras and webcams to display images should also be highlighted.

16 CULTURE

The way that some students use the Internet can lead to depersonalisation (forgetting that in the virtual world, there is a real person) and this can lead to cyber bullying, which can become far more extreme and wide-ranging than 'face to face' bullying.

17 COMMERCE

Students shall be protected from and educated about issues surrounding commercial marketing such as spam, phishing etc.

18 ASSESSING RISKS

Some material available through the Internet is unsuitable for students. The school takes all reasonable precautions to ensure that users access only appropriate material. However, due to the nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

Access to any websites involving gambling, games or financial scams is strictly forbidden and shall be dealt with accordingly.

19 INTRODUCING THE E-SAFETY POLICY TO STUDENTS

- Students are informed that Internet use is only with adult supervision.
- Pupils are informed that internet use will be closely monitored, and that misuse will be dealt with appropriately.
- Pupils are instructed in responsible and safe use before being allowed access to the Internet.

- Lessons on e-safety and responsible Internet use, covering both school and home use, are taught.

20 STAFF AND THE E-SAFETY POLICY

- All staff are given the school e-safety policy and its importance explained.
- Staff are made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Staff shall not use personal email or mobile technology to contact students. If contact is necessary, a school telephone / email account shall be used.
- It is essential that teachers and learning support staff are confident about using the internet in their work and shall be given opportunities to discuss issues and develop appropriate teaching strategies.
- All new staff are given a copy of the policy during their induction.
- Staff development in safe and responsible use of the internet shall be provided as required.

21 PARENT/CARERS SUPPORT

- Parents/carers are informed of the School's Internet Policy which can be accessed on the school website.
- Parents' attention is drawn to the school e-safety Policy in newsletters.
- Any issues concerning the internet shall be handled sensitively to inform parents/carers without undue alarm.
- Parents and carers shall from time to time be provided with additional information on e-safety.
- The school requires all new parents to sign the parent/ pupil agreement when they register their child with the school.
- Periodically parent workshops are held to update awareness on e-safety.

22 HANDLING E-SAFETY COMPLAINTS

- Pupils and parents are informed of the complaint's procedure.
- They are informed of how and where to report incidents.
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Complaints of Internet misuse is dealt with by SLT.
- Any complaint about staff or pupil misuse shall be referred to SLT/GB immediately.

- Parents/carers and pupils work in partnership with school staff to resolve any issues.
- Sanctions within the school discipline policy include:
    - Interview by a member of SLT.
    - Informing parents or carers.
    - Removal of Internet or computer access for a period.

23 ROLES AND RESPONSIBILITIES

SLT ensure that:

- All staff and volunteers understand and are made aware of the school's eLearning/Safety Policy and arrangements.
- Staff understand that misuse of the internet may lead to disciplinary action and
- possible dismissal.
- All staff are included in e-Safety training.
- A commitment to e-Safety is an integral part of the safer recruitment and
- selection process of staff and volunteers.
- ICT security is maintained.
- Staff attend appropriate training.
- Support and training for staff and volunteers on e-Safety is provided.
- The school's ICT systems are regularly reviewed with regard to security.
- Virus protection is regularly reviewed and updated.
- Regularly check files on the school's network.
- The Governing Body of the school will ensure that:
- There is a senior member of the school's leadership team who is designated to
- take the lead on E-Learning/Safety within the School.
- Procedures are in place for dealing with breaches of e-safety and security and
- are in line with Local Authority procedures.
- All staff and volunteers have access to appropriate ICT training.