E SAFETY AND SOCIAL MEDIA POLICY

Board of Trustees Approved: February 2021

Date of next review: February 2022

Reviewed by: The Principal and the Teaching and Learning Committee

This policy will be reviewed every year and at every review the policy will be shared with the full Board of Trustees.

General definitions

Throughout this policy, *Wynstones* means Wynstones school and will be used interchangeably with s*chool* and *the school; parents* includes guardians, carers and those with parental responsibility for children entering the school; s*tudents* will be used throughout.

Regulatory and publication context

Independent schools are not required to have a website, but are required to make policies and information available to parents upon request, in line with the Education (Independent School Standards) Regulations 2014.

Wynstones systematically chooses to publish its policies online, in order to enable ease of access for parents, and to participate in the wider social discourse on appropriate, effective and fair educational provision.

Policy Contents

1 Introduction

At Wynstones we are dedicated to nurturing each child's capacity for creative imagination, independent thinking and positive action, and believe that below the age of 12 we should limit the access to information technology within the school setting. In kindergarten and in the early years of the school we advise parents that access to information technology is largely unnecessary.

We encourage parents/carers to keep an open dialogue with their children, other class parents/carers and teachers regarding digital media. Specifically, parents/carers should speak to teachers, either privately or with other parents in class or other group meetings, about their questions and challenges related to digital media so that together they can work out viable approaches.

Wynstones will deal with such incidents within this policy and associated 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.

2 Access to the Internet

At Wynstones, students are sometimes allowed internet access in school at the discretion of the teacher to help in studies. We are aware that many students will have access to such technologies at home by this age.

The use of the internet can put young people at risk within and outside the school. Some of the dangers they may face include:

- 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
- 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 health and physical, social and emotional development and learning of the young person.

When young people are using computers they are to be sited in areas of high visibility which will enable young people to be closely supervised and their online use to be appropriately monitored.

3 Education

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' 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.

Wynstones will ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

Staff alongside parents/carers, should consider it to be their duty to make children and young people aware of the potential risks associated with online technologies. This will empower them with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.

Staff should reinforce e-safety messages in the use of ICT to all students when using computers with them.

This policy applies to all staff and students and anyone using the school internet system.

4 Advice for students

- Don't publish identifying information.
- Pick a user name that doesn't include any personal information.
- Set up a separate email account that doesn't use your real name and use that to register and receive mail from social media sites. That way if you want to shut down your connection, you can simply stop using that mail account.
- Only use your school email account to communicate with your teachers.
- Use a strong password (at least 8 characters; mixture of lower case letters, upper case letters, numbers and symbols).
- Keep passwords safe, and change them regularly.
- Set social media privacy setting to be private, not public.
- Only allow people you know in real life to view your profiles on social media.
- What goes online stays online. Don't say anything or publish pictures that might cause you or anyone else embarrassment later. If you wouldn't say it to your parents, don't say it online!
- Be on your guard.
- Talk to parents/carers if you feel uncomfortable.
- Save or print evidence

5 Advice for parents/carers

- Set ground rules. Discuss. Continue to talk.
- Limit the amount of time online.
- Use ISP filtering.
- Set up a family e-mail account for registering on websites, competitions etc.
- Monitor online activity (recently visited sites, click the History button).
- Software for filtering isn't fool proof - combine with supervision.
- Check temporary files (open Internet Explorer and select Internet Options, on the General tab under Temporary Internet Files, click the Settings button and the click View Files).
- Contact CEOP or the police if you suspect grooming.

CEOP (Child Exploitation & Online Protection) is dedicated to eradicating the sexual abuse of children, and is affiliated to the Serious Organised Crime Agency (SOCA).

6 Safer search engines

- surfsafely.com
- askkids.com
- yahookids.com

7 Further information and advice

- childnet.com (select 'Know It All' for a wide range of links to other sites)
- google.co.uk/goodtoknow (select 'Stay safe online')
- getsafeonline.org
- kidscape.org.uk

Useful information can also be found at: https://www.gov.uk/government/publications/preventing-and-tackling-bullying

8 Control Measures

The following control measures will be put in place which will manage internet access and minimise risk:

- Secure broadband or wireless access.
- A secure, filtered, managed internet service provider and/ or learning platform.
- Secure email accounts.
- Regularly monitored and updated virus protection.
- A secure password system.
- An agreed list of assigned authorised users with controlled access.
- Clear Acceptable Use Agreement

9 Social Networking

It is to be recognised that staff are also likely to use social networking sites in their recreational time on their own personal computers. This form of activity is not to be discouraged however staff must

agree and adhere to the e-Safety and Social Media Policy. It must be ensured that the use of such sites will not compromise professional integrity or bring the school into disrepute.

It must be recognised that social networking sites and mobile technologies can be used for negative and anti-social purposes. Cyberbullying, for example, is to be considered as unacceptable as any other form of bullying and will be handled in accordance with the Anti Bullying Policy.

Social media and social networking sites play an important role in the lives of many young people. We recognise that websites can bring risks, but equally there are many benefits to be reaped. This document gives clarity to the way in which social media are to be used by students and school staff at Wynstones.

There are five key areas:

1. a) There will be no access to social media sites for students in Lower School at any time.
   b) Classes 9 and 10 will only have access to social media if authorised by a teacher within a lesson.
2. Use of social networking by staff in a personal capacity
3. Creation of network accounts by staff for use in education
4. Comments posted by parents/carers
5. Dealing with incidents of online bullying

It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.

10 Procedures issued to staff

- Staff must never add a student as a 'friend' or contact on any personal social networking medium.
- Staff must not use social networking sites within school times.
- Staff should review and adjust their privacy settings to give them the maximum level of privacy and confidentiality.
- Staff must not post any comments about the school, students, parents or colleagues (including Trustees).

Inappropriate use by staff should be referred to Vice Principal (DSL) or other member of the Senior Leadership Team (SMT) in the first instance.

11 Creation of network accounts by staff for use in education

- All social media services must be approved by the school SMT in advance of any educational work being undertaken.

12 Comments posted by parents/carers

- Parents/carers will be made aware of their responsibilities regarding their use of social networking.
- Parents/carers should not post pictures of students other than their own children on social networking sites.
- Parents/carers should raise concerns or make complaints through official school channels (see the Complaints Policy) rather than posting them on social media. Parents/carers should not post malicious or fictitious comments on social networking sites about any member of the school community

- Any comments on social media sites that could be interpreted as bringing the school into disrepute will be referred to legal experts for who will advise on an appropriate course of action.

13 Dealing with incidents of online bullying or inappropriate behaviour

The school can take action against incidents that happen outside school if it:

- Poses a threat to another Student or member of the public or
- Could have repercussions for the orderly running of the school or
- Could adversely affect the reputation of the school.

Use of social networking sites to harass, bully or intimidate would be covered by this irrespective of when/where the post was made.

This policy should be read in conjunction with the IT Policy, Behaviour, Anti-bullying, and Safeguarding and Child Protection policies

14 Should an e-safety incident occur

Please contact Vice Principal (DSL): kdeferrer@wynstones.com or the Director of Finance and Resources: awelsh@wynstones.com