E Safety policy

This should be read in conjunction with the IT, Digital Devices & Student Acceptable Use Policy, Staff Acceptable Use Policy and Social Media Policy
as well as Behaviour, Anti-bullying, and Safeguarding and Child Protection policies

Should an e-safety incident occur please contact:

Designated Child Protection & Safeguarding Lead:
Marianne Law-Lindberg 01452 429206, 07768 870671
mglaw-lindberg@wynstones.com

Deputy Designated Child Protection & Safeguarding Lead:
Rebekah Hoyland 01452 429226, 07721 718511 rhoyland@wynstones.com
safeguarding@wynstones.com

If they are not available, contact: **Local Authority Designated Officer's** (LADO):
Nigel Hatten 01452 426994 Georgina Summers 01452 426320
The LADO on duty can also be contacted on 07717 571801

Introduction

Digital technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

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 question the positive benefits to be gained from information technology. In kindergarten and in the early years of the lower school we advise parents that access to information technology is largely unnecessary, just as we suggest that television viewing should be limited.

We encourage parents to keep an open dialogue with their children, other class parents and teachers regarding digital media. Specifically, parents 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.

Access to the Internet

At Wynstones School pupils in Upper School 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
- Cybersquatting
- 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 children are using computers they are to be sited in areas of high visibility which will enable children, young people and adults to be closely supervised and their online use to be appropriately monitored.

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

Staff alongside parents and 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.

'E-safety' will taught to students in the Upper School. Staff should reinforce e safety messages in the use of ICT to all pupils when using computers with them.

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

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

Advice for parents

- 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).

Safer search engines:

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

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

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

Social Networking (also see Social Media Policy)

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 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.

Staff must not have a pupil as a 'friend' or contact on any social networking medium.

Issue Date: November 2017	**Review Date:** Michaelmas Term 2018/2019
Authorised by: **Name:** **Job title:**	**Sign:**
Date:	