WYVERN COLLEGE
ONLINE SAFETY POLICY

Date of last revision.	March 2021 (Head of Pastoral).
Date reviewed and ratified by Care, Guidance and Support Committee.	22nd March 2021.
Date of next review.	March 2022.

A. Purpose and rationale

1. Wyvern College aims to have robust processes in place to ensure the online safety of students, staff, volunteers and Trustees; to deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology; to establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
2. This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:
   - Teaching online safety in schools
   - Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
   - Relationships and sex education
   - Searching, screening and confiscation
3. It also refers to the DfE's guidance on protecting children from radicalisation.
4. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.
5. The policy also takes into account the National Curriculum computing programmes of study.

B. Principles and content

1. This policy has been written in consultation with the Wyvern College Senior Leadership Team and the Network Manager.
   - This policy is available on the College website;
   - Trustees will ensure the policy is reviewed every three years;
   - All staff will be made aware of this policy.

C. Educating students about online safety

1. Students will be taught about online safety as part of the curriculum.
2. In **Key Stage 3**, students will be taught to:
   - Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy;

- Recognise inappropriate content, contact and conduct, and know how to report concerns.

3. Students in **Key Stage 4** will be taught:
    - To understand how changes in technology affect safety, including new ways to protect their online privacy and identity;
    - How to report a range of concerns.
4. By the **end of secondary school**, students will know:
    - Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online;
    - About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online;
    - Not to provide material to others that they would not want shared further and not to share personal material which is sent to them;
    - What to do and where to get support to report material or manage issues online;
    - The impact of viewing harmful content;
    - That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners;
    - That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail;
    - How information and data is generated, collected, shared and used online;
    - How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

D. Educating parents about online safety

1. Wyvern College will raise parents' awareness of internet safety in regular communications home such as the monthly parental online safety newsletter and in information via our website.
2. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the relevant Pastoral Leader or a member of the College's safeguarding team.

E. Cyber-bullying

1. Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

F. Preventing and addressing cyber-bullying

1. To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
2. The College will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
3. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
4. In relation to a specific incident of cyber-bullying, the College will follow the processes set out in both the behaviour and bullying policies. Where illegal, inappropriate or harmful material has been spread among students, the College will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

G. Examining electronic devices

1. School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images

or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. At Wyvern College, searches of electronic devices are carried out by members of the safeguarding team only.

2. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

   - Cause harm, and/or
   - Disrupt teaching, and/or
   - Break any of the College rules

3. If inappropriate material is found on the device, it is up to the lead safeguarding member of staff to decide whether they should:

   - Delete that material, or
   - Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
   - Report it to the police.

4. Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.

5. Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the Wyvern College complaints procedure.

H. Students using mobile devices in College

1. Students may bring mobile devices into College and are only permitted to use them in line with the College's mobile phones policy.

2. Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the College behaviour policy, which may result in the confiscation of their device.

I. Staff using work devices outside school

1. All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

   - Keeping the device password-protected – Wyvern's password policy requires at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol). You cannot use any 3 or more consecutive letters from your name and surname and you cannot use a password you have used in your previous 10 passwords.
   - Ensuring their hard drive encryption password remains protected – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
   - Making sure the device locks if left inactive for a period of time.
   - Not sharing the device among family or friends.
   - Maintaining anti-virus and anti-spyware software and definition updates.
   - Keeping operating systems up to date – always install the latest updates.

2. Work devices must be used solely for work activities.

3. If staff have any concerns over the security of their device, they must seek advice from the Network Manager.

J. How Wyvern College will respond to issues of misuse

1. Where a student misuses the College's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

2. Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

3. The College will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

K. Responsibility for implementation

Staff

1. It is the responsibility of all staff in College to be aware of this policy. Staff receive annual updates and training where appropriate. Staff are responsible for implementing this policy consistently and agreeing and adhering to the terms on acceptable use of the College's ICT systems and the internet ensuring that pupils follow the College's terms on acceptable use. Staff will work with the safeguarding team to ensure that any online safety incidents are reported immediately and that any incidents of cyber-bullying are dealt with appropriately in line with the College behaviour policy.

The Headteacher

2. The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the College.

The Designated Safeguarding Lead

3. Details of the Wyvern College's Designated Safeguarding Lead (DSL) are set out in our child protection and safeguarding policy. The DSL takes lead responsibility for online safety in College, in particular:

    - Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the College;
    - Working with the Headteacher, Network Manager and other staff, as necessary, to address any online safety issues or incidents;
    - Ensuring that any online safety incidents are recorded and dealt with appropriately in line with this policy;
    - Ensuring that any incidents of cyber-bullying are recorded and dealt with appropriately in line with the College behaviour policy;
    - Updating and delivering staff training on online safety;
    - Liaising with other agencies and/or external services if necessary
    - Providing regular reports on online safety in College to the Headteacher and Trustees.

Trustees

4. The Trustees have overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The Care, Guidance & Support (CG&S) Trustees will discuss online safety with the Designated Safeguarding Lead (DSL) through their programme of regular meetings.

The Network Manager

5. The Network Manager is responsible for:

    - Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at College, including terrorist and extremist material;
    - Ensuring that the College's ICT systems and electronic data are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
    - Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
    - Ensuring that any online safety incidents are recorded and passed to the Designated Safeguarding Lead and Deputy Designated Safeguarding Leads on the Senior Leadership Team

L. Accountability

1. This policy is drafted by the Pastoral Assistant Headteacher. It is the responsibility of the Pastoral Assistant Headteacher to ensure that the policy is available on the College website for parents and other stakeholders.

M. Supporting documents

2. This document should be read in conjunction with the College's:

- Child protection and safeguarding policy (including the PREVENT agenda)
- Behaviour policy
- Preventing Bullying policy
- Sex and Relationships policy
- Staff disciplinary procedures (including the staff code of conduct)
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: ICT acceptable use agreement (students and parents)

ACCEPTABLE USE OF THE WYVERN COLLEGE ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS

I will read and follow the rules in the acceptable use agreement policy

When I use the College's ICT systems (like computers) and use the internet in College I will:

- Always use Wyvern's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent
- Follow the online PRIDe expectations at all times, including when I am taking part in a live Teams lessons
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Report any incidents of cyber-bullying to a trusted adult
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Participate in any incidents of cyber-bullying
- Log in to Wyvern's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent, or without adult supervision

If I bring a personal mobile phone into College:

- I will only use it in line with the College's mobile phones policy
- If I am given specific permission to use my phone, I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that Wyvern College will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (student):	**Date:**
Parent agreement: I agree that my child can use Wyvern College's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the College's ICT systems and internet, and for mobile phones in College, and will make sure my child understands these.	
Signed (parent):	**Date:**