Yarlet School Online Safety and Acceptable Use Agreement (AUA) Policy

1. Aims

The aim of this policy is to ensure that teachers/practitioners, volunteers, parents and pupils have a clear and agreed understanding of the benefits and risks of online safety. It provides advice on acceptable use and effective control measures to enable individuals to use ICT resources in a safe online environment. We aim to deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology and establish clear mechanisms to identify, intervene and escalate an incident, where appropriate. Creating a safer online environment is on-going, so clear monitoring, evaluation and review of procedures are essential.

2. Legislation and guidance

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 Headmasters and school staff
- [Relationships and sex education
- Searching, screening and confiscation
- protecting children from radicalisation.

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 pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Headmaster to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

3.2 The Headmaster

The Headmaster is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL, DDSL and DDDSL are set out in our Safeguarding Children Policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular, ensuring this policy is an up to date, working document.

3.4 All staff and volunteers

All staff, including contractors and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 Parents

Parents are expected to:

- Notify a member of staff or the Headmaster of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (see appendix 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites as well as the school's dedicated online safety information page (www.yarletschool.uk/index.php/keeping-safe-online):

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum following the guidance in:

- National Curriculum computing programmes of study.
- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Pre Prep**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In **Forms 3 - 6** pupils will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not.*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

In **Forms 7 and 8**, pupils 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

*By the **end of KS3**, they 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 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*

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies, tutor time and PSHE lessons to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in our regular monthly internet safety letter or other communications home, in information via our dedicated Online Safety page on our website (www.yarletschool.uk/index.php/keeping-safe-online), or Internet Safety talks for parents' evenings. This policy will also be available for parents via our website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headmaster and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headmaster.

6. Cyber-bullying

6.1 Definition

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. (See also the school behaviour policy and Bullying Policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Through computing lessons, tutor time and assemblies the school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

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.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school 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.

6.3 Examining electronic devices

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.

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 school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team 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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school (AUA)

All pupils, parents, staff, volunteers (when necessary) are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. Pupils do not access social media sites within school time. Pupils do not use e-mailing as a form of communication except in exceptional circumstances when they are e-mailing as part of a teacher-led activity (such as contacting an e-mail address as part of Literacy/ computing, for example). When using the internet, to minimize any risks, school computers have security settings which prohibit pupils from accessing unsuitable sites.

8. Pupils using mobile devices in school

Pupils are not permitted to use mobiles whilst in school. If a mobile is brought into school, it must be handed into the Deputy for safe keeping during the day, then collected at the end of the day.

Mobiles may occasional be brought in for special occasions, such as Wednesday afternoon clubs or a Boarding Activity. If so, the mobile must be handed into the Deputy in the morning.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 2).

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

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. Safeguarding children who work from home

It is important that all staff who interact with children, including online, continue to look out for signs of when a child may be at risk. Any such concerns should be dealt in accordance with the procedures set out in this and the school's safeguarding policy and where appropriate referrals should still be made following the correct protocol. Online teaching should follow the procedures and principles as set out in Yarlet School's Code of Conduct and Video Conferencing Usage Agreement. Yarlet School will ensure that any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

11. How the school will respond to issues of misuse

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

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 handbook (code of conduct). The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An example incident report log can be found in appendix 3.

We are aware of the need to monitor online safety very carefully, and to review it regularly, so that we can take account of new, developments in technology or changes to the physical environment of the school. We will therefore review this policy every two years, or earlier if necessary.

Signed:

Ian Raybould, Headmaster and DSL

Date: November 2020

Review: November 2022

Appendix 1: Acceptable use agreement (staff, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, VOLUNTEERS AND VISITORS	
Name of staff:	
• I understand, accept and agree to adhere to Yarlet's online safety policy • I understand it is my responsibility to ensure safe and responsible use of ICT within Yarlet School • I understand that Yarlet's ICT systems are primarily intended for educational use • I will not engage in any online activities that may compromise my professional responsibilities • I will only use Yarlet's official system in a professional tone and manner • I understand that if I fail to comply with this AUA I could be subject to disciplinary action • I will not bring Yarlet's name into disrepute • I will observe confidentiality and refrain from discussing any issues relating to work • I will not share or post in an open forum any information that I would not want Staff, Volunteers, Parents or Pupils to view • I will keep my professional and personal life separate and not accept pupils as 'friends' on Social Media • Although the practice of teachers, adult volunteers and parents becoming online 'friends' on social media has existed historically, this is now discouraged and is being phased out. • I will consider how my social conduct may be perceived by others and how this could affect my own reputation and that of Yarlet • I will either avoid using a profile photograph or ensure it is an image I would be happy to share with anyone • I will report any known breaches of the above to the Headmaster, Mr. Raybould or Deputy Head, Mrs Burrows-Berry • I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to Mr. Raybould or Mrs Burrows-Berry	
Signed (staff):	**Date:**

Appendix 2: Acceptable use agreement for pupils and parents/carers

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
As part of your child's curriculum and the development of computing skills, Yarlet School is providing supervised access to the Internet in computing. We believe that the use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use, and sign and return the consent form so that your child may use Internet at School. Although there may be concerns about pupils having access to undesirable materials, we have taken positive steps to deal with this risk in school. A filtering system will be in operation that restricts access to inappropriate materials, and all sessions involving use of the Internet will be monitored by a member of staff. In addition, we will be delivering an Internet Safety Programme for all pupils which teaches the safe and appropriate behaviour to adopt when using the Internet, e-mail and other technologies. Each member of staff and each student using the Internet must agree to follow an Acceptable Use Policy. These policies set out the rules which must be adhered to, for the protection of all users. Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature of content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.	
The school computer system provides Internet access to Pupils and Staff. These rules will help us to be fair to others and will keep everyone safe. • I will ask permission before entering any web site unless my teacher has already approved that site. • I will use only my own login and password, which I will keep secret. • I will not look at or delete other people's files. • I will only e-mail people I know, or whom my teacher has approved. • The messages I send will be polite and sensible. • When sending e-mail, I will not give out my home address or phone number or arrange to meet someone. • I will ask permission before opening an e-mail or an e-mail attachment sent by someone I do not know. • I will not use Internet chat or any social networking sites. • If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately. • I know that the school may check my computer files and may monitor the Internet sites I visit. • The school ICT systems may not be used for private purposes unless the Headmaster has given permission for that use. • I understand that if I deliberately break these rules, I would be stopped from using the Internet or computers. The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mail and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**