At Havelock children and staff believe that we all have the right to be educated and play in a safe and secure environment. The Rights Ambassadors and School Council have been involved in reviewing our policy so that the children are at the heart of decision making at Havelock. As a Rights Respecting School we uphold the following Articles from the UNCRC linked to online safety. 

**Article 2:** Every child has the right to be treated fairly and with respect.

**Article 12** (respect for the views of the child) 
Every child has the right to say what they think in all matters affecting them, and to have their views taken seriously.

**Article 19:** Every child has the right to be protected from harm.

**Article 23:** A child with disability has the right to live a full and decent life in conditions that promote dignity, independence and an active role in the community.

**Article 28:** Every child has the right to an education.

1. **Aims**

Our school aims to:
• Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
• Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
• Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education’s statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department’s guidance on 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.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher 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).

The governor who oversees online safety is Mr Michael Keller

All governors will:

• Ensure that they have read and understand this policy
• Agree and adhere to the terms on acceptable use of the school’s ICT systems and the internet (appendix 2)

3.2 The headteacher

The headteacher 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 designated safeguarding lead (DSL team): J Bailey, H Rupra and C Rees are set out in our child protection and safeguarding policy.

The DSL team takes lead responsibility for online safety in school, in particular:

• Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
• Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
• Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
• Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
• Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
• Liaising with other agencies and/or external services if necessary
• Providing regular reports on online safety in school to the headteacher and/or governing board

3.4 The ICT manager

The ICT Network Yosabe System - Soloman Yosabe/Olu Oluseye managers is responsible for:
• Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
• Ensuring that the school’s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
• Conducting a full security check and monitoring the school’s ICT systems on a fortnightly basis
• Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
• Ensuring that any online safety incidents are logged (see appendix 4) 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 appendix 6

3.5 All staff and volunteers

All staff, including contractors and agency staff, 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 (appendix 2), and ensuring that pupils follow the school’s terms on acceptable use (appendix 1)
• Working with the DSL to ensure that any online safety incidents are logged (see appendix 4&6) 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

3.6 Parents

Parents are expected to:
• Notify a member of staff or the headteacher 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 (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:
• What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
• Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

3.7 Visitors and members of the community
Visitors and members of the community who use the school’s ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, 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

Pupils in **Key Stage 2** 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

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

The school will use assemblies 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 letters or other communications home, and in information via our website, workshops with the SLT and ICT leader, messages sent via the school app. This policy will also be shared with parents.

Online safety will also be covered during parents’ evenings.

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

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

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.)

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.

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. Teachers will discuss cyber-bullying with their class, and the issue will be addressed in assemblies.

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 (see section 11 for more detail).
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/anti bullying 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. (Appendix 4)

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

All pupils, parents, staff, volunteers and governors 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.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

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, as set out in appendix 2.3.

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. Any USB devices containing data relating to the school must be encrypted.

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. 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 the behaviour policy. 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 disciplinary procedures. 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.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 6.

This policy will be reviewed by the DSL team. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

<table>
<thead>
<tr>
<th>Draft</th>
<th>March 2019 H Rupra</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adopted</td>
<td>March 2019</td>
</tr>
<tr>
<td>To be reviewed</td>
<td>March 2020</td>
</tr>
</tbody>
</table>
## Appendix 1:

### Havelock Primary School & Nursery

#### Acceptable use of the school’s ICT systems and internet: agreement for pupils and parents/carers

<table>
<thead>
<tr>
<th>Name of pupil:</th>
</tr>
</thead>
</table>

**When using the school’s ICT systems and accessing the internet in school, I will not:**

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher’s permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- 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
- Share my password with others or log in to the school’s network using someone else’s details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher’s permission
- 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 the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school’s ICT systems and internet responsibly.

<table>
<thead>
<tr>
<th>Signed (pupil):</th>
<th>Date:</th>
</tr>
</thead>
</table>

**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.

<table>
<thead>
<tr>
<th>Signed (parent/carer):</th>
<th>Date:</th>
</tr>
</thead>
</table>
## Acceptable Use Agreement: Staff, Governors Volunteers and Visitors

### Acceptable Use Agreement / Code of Conduct

#### Acceptable use of the school’s ICT systems and the internet: agreement for staff, governors, volunteers and visitors

<table>
<thead>
<tr>
<th>Name of staff member/governor/volunteer/visitor:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

When using the school’s ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school’s reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school’s network using someone else’s details

I will only use the school’s ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school’s data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school’s ICT systems and internet responsibly, and ensure that pupils in my care do so too.

<table>
<thead>
<tr>
<th>Signed (staff member/governor/volunteer/visitor):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date:</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
LAPTOP/iPad AGREEMENT FOR STAFF

This agreement is between:
HAVELOCK PRIMARY SCHOOL & NURSERY and ____________________________
(staff name)

The following are the conditions under which you accept the provision of a laptop for your use from the School. This Agreement will start on receipt of the laptop from the School. The school reserves the right to transfer the laptop to another eligible member of staff if you do not, or are unable to, for any reason fulfil the requirement of this Agreement.

Under this Agreement the School will:

1. Set up the laptop/iPad to enable you to connect to and make effective use of the school network and provide a secure location for the safe storage of your laptop/iPad during the school day.
2. Plan and manage the integration of laptops/iPads into the school environment, and provide the professional development required to enable you to use the laptop/iPad effectively in your professional practice.
3. Insure the laptop/iPad against loss or damage whilst on the school premises or being used for school purposes outside the school environment provided that the damage or loss is not sustained as a result of the member of staff’s negligence.
4. Have an expectation that you will abide by the School’s Responsible Use.

Under this Agreement You will:

1. Use the laptop/iPad for the purposes it was provided and abide by the School’s Acceptable Use Policy.
2. Provide suitable care and security of the laptop/iPad computer at all times and immediately report any damage or loss of the laptop/iPad to the Headteacher.
3. Be responsible for repair/replacement costs of the laptop/iPad where the loss or damage is as a result of your own negligence.
4. Make a commitment to achieving the Computing goals of the school and take part in the Computing professional development activities provided for you by the School.
5. Make necessary arrangements, for the return of the laptop/iPad to the School when you resign or leave the school of when you will be away from the school for an extended period.
6. In accordance with school policies, be held responsible for any involvement by yourself or any other user of your laptop/iPad in activities associated with accessing inappropriate or illegal materials.
(staff name) accepts the conditions, as outlined in the Laptop/iPad Agreement, for provision of a laptop/iPad by

HAVELOCK PRIMARY SCHOOL & NURSERY
You have been provided with a _______________________ laptop
(model)

The serial number for this laptop is: _______________________

You have been provided with a _______________________ ipad
(model)

The serial number for this laptop is: _______________________

I also confirm that I have read and understood Havelock Primary School’s Acceptable Use Policy.

Signed: ___________________________ Date: ____________
(Staff name)

Signed: ___________________________ Date: ____________
(Headteacher)
Appendix 4

Staff Response to an E-Safety Incident of Concern:

If a child is at immediate risk
- Follow the school’s child protection procedures, informing the school Child Protection Lead
- Contact Police 999

If in immediate danger...
(E.g. child going to meet someone they’ve met online)
- Contact 경찰 999

If in imminent danger...
(E.g. planning to meet someone they have met online)
- Contact ECIRS

Illegal/Harmful Activity or Material found/suspected
(E.g. grooming, child online sexual exploitation, high end cyberbullying: serious threats, inappropriate sexual chat or conduct, pressure to send images, sexting)
- Confiscate any devices involved to retain evidence as per school procedures
- Refer to Social Care via your designated Child Protection Lead
- Refer to ECRS or any allocated social worker via the school’s designated Child Protection Lead
- Contact UK Safer Internet Centre Helpline to report/remove inappropriate content

Inappropriate Activity or Material found/suspected
(E.g. Peer-related threats/harassment, hacking, creating fake accounts, circulating offensive messages/photos/videos)
- Confront any schools involved as per school procedures
- Contact ECRS and decide with them if Police CP Team need to be informed
- Keep any evidence (e.g. screenshots, emails)
- Inform parents/carers
- Institute restorative approaches

e-Safety Incident occurs
- Unsure? Contact Local Authority Child Protection Advisors

1. Report to Headteacher
2. Report to LADO within 1 day (as per statutory requirement)
3. Contact ECIRS and decide with them if Police CP Team need to be informed
4. Keep any evidence (e.g. screenshots, emails)
5. Record in School’s e-Safety log
6. Inform parents/carers
7. Institute restorative approaches

Instigator:
- Support/advice from e-Safety Coordinator
- Review incident and identify if other pupils were involved
- Decide on appropriate sanctions based on school rules/policies
- Training/restorative justice
- Review School Procedures to develop best practice

Victim:
- Support/advice from e-Safety Coordinator
- School support, e.g. counselling
- Peer mentoring
- Update parents/carers

Whole School Action:
- Review school policies & procedures to develop best practice
- Staff Training

Useful School Contacts:
- Child Protection Officer:
- E-Safety Coordinator:
- Safer School Officer:
- Child Protection Advisors
- Other details:

External Contacts as a Resource
- ECIRS (Ealing Children’s Integrated Response Service) – 020 8825 8000
- Local Authority Child Protection Advisors – 020 8825 8268/8232/9316/8404
- LADO (Local Authority Designated Officer) 020 8825 8930
- ClickCEOP – Parents & pupils can contact CEOP directly if child is in immediate risk
  - UK Safer Internet Centre Helpline – 0844 381 4772
### Online safety training needs audit

<table>
<thead>
<tr>
<th>Question</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of staff member/volunteer:</td>
<td></td>
</tr>
<tr>
<td>Do you know the name of the person who has lead responsibility for online safety in school?</td>
<td></td>
</tr>
<tr>
<td>Do you know what you must do if a pupil approaches you with a concern or issue?</td>
<td></td>
</tr>
<tr>
<td>Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?</td>
<td></td>
</tr>
<tr>
<td>Are you familiar with the school's acceptable use agreement for pupils and parents?</td>
<td></td>
</tr>
<tr>
<td>Do you regularly change your password for accessing the school's ICT systems?</td>
<td></td>
</tr>
<tr>
<td>Are you familiar with the school's approach to tackling cyber-bullying?</td>
<td></td>
</tr>
<tr>
<td>Are there any areas of online safety in which you would like training/further training? Please record them here.</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 6:

<table>
<thead>
<tr>
<th>Date</th>
<th>Where the incident took place</th>
<th>Description of the incident</th>
<th>Action taken</th>
<th>Name and signature of staff member recording the incident</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>