Online safety policy



**(in draft form until discussed fully at management board 29th Oct)**

Signature Z. Stevenson Headteacher Date: 10/21

Signature Chair of management board Date:

**The minutes of the Management Board (To be discussed by 29th Oct) clearly demonstrate where this Policy has been developed with the staffing group using their expertise and knowledge.**

**Contents**

1. Aims 2

2. Legislation and guidance 2

3. Roles and responsibilities 3

4. Educating pupils about online safety 4

5. Educating parents about online safety 5

6. Cyber-bullying 5

7. Online hoaxes 6

8. Acceptable use of the internet in school 6

9. Pupils using mobile devices in school 6

10. Staff using work devices outside school 7

11. How the school will respond to issues of misuse 7

12. Training 7

12. Monitoring arrangements 7

13. Links with other policies 7

Appendix 1: acceptable use agreement (pupils and parents/carers) 9

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors) 10

Appendix 3: online safety training needs – self-audit for staff 11

**…………………………………………………………………………………………………………………………….**

# 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 2021](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2), and its advice for schools on [preventing and tackling bullying](https://www.gov.uk/government/publications/preventing-and-tackling-bullying) and [searching, screening and confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation). It also refers to the Department’s guidance on [protecting children from radicalisation](https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty).

It reflects existing legislation, including but not limited to the [Education Act 1996](https://www.legislation.gov.uk/ukpga/1996/56/contents) (as amended), the [Education and Inspections Act 2006](https://www.legislation.gov.uk/ukpga/2006/40/contents) and the [Equality Act 2010](https://www.legislation.gov.uk/ukpga/2010/15/contents). In addition, it reflects the [Education Act 2011](http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted), 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.

 This policy complies with our funding agreement and articles of association.

# 3. Roles and responsibilities

**3.1 The Management Board**

The Management Board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Management 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 board member who oversees online safety is Darryl Gough.

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) Laurence Morris, DDSLs Zoie Stevenson, Sarah Gould and Tom Morris are set out in our child protection and safeguarding policy.

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

* Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
* Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents
* Ensuring that any online safety incidents are logged on My Concern 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 according to self audit completed and My Concern audit (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

This list is not intended to be exhaustive.

**3.4 The ICT manager**

The ICT manager 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 including ‘Senso’ on a daily 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 on My Concern 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
* Ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
* Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
* Examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

This list is not intended to be exhaustive.

**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 on My Concern 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.

**3.6 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>
* Online safety <https://www.thinkuknow.co.uk/>

**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

All pupils will be taught throughout the curriculum via assembly, tutor times, PSHE, ICT tech, drop down days and the and the wider curriculum:

* 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 a range of concerns
* To recognise and report online bullying

# 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

This policy will also be shared with parents.

Online safety will also be covered via ongoing parental contact.

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

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. Class teachers/form teachers and Keyworkers will discuss cyber-bullying with their tutor groups, 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. 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](https://www.gov.uk/government/publications/searching-screening-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. Online Hoaxes**

This is written in light of DFE guidance <https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes>

A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge. We need to ensure that pupils are able to remain safe on the Internet and to help them recognise what is true and what is not. As with all safeguarding issues, we will ensure that all pupils know who to speak to if they have a concern.

If school is made aware of a potential online hoax, we will undertake a case-by-case assessment, establishing the scale and nature of the possible risk to our children and young people, The DSL will check the factual basis of any harmful online challenge or online hoax with a known, reliable and trustworthy source, such as the Professional Online Safety Helpline from the UK Safer Internet Centre. Where harmful online challenges or online hoaxes appear to be local (rather than large scale national ones) local safeguarding advice, such as from the local authority or local police force, may also be appropriate and helpful.

**7.1 Whether to make pupils and parents/carers aware of issues**

If this the issue relates to an online hoax, it is generally better not to raise awareness of it as this can spread the hoax further and lead to unnecessary anxiety. It will generally be better to talk about hoxes in non-specific terms and to offer support to any students who we know have been upset by it.

The school response will be measured in these terms:

* is it factual?
* is it proportional to the actual (or perceived) risk?
* is it helpful?
* is it age and stage of development appropriate?
* is it supportive?

# 8. 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.

# 9. Pupils using mobile devices in school

All KS3/4 pupil belongings including mobile phones must be kept in the office in pupils’ personal tray.

Sixth form pupils are allowed to use mobile devices in designated areas and at set times. Abuse of this will mean the privilege is lost.

On occasion pupils maybe allowed their personal devices and phones when using school transport or educated of site.

# 10. 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.

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.

# 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 the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

We will ensure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account.

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.

# 12. 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 and deputies 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 reviews behaviour and safeguarding issues related to online safety on My Concern

This policy will be reviewed yearly by the DSL and DDSL. 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
* Positive Engagement Policy
* Staff Disciplinary Procedures
* Data Protection Policy and privacy notices
* Complaints Procedure
* Peer on Peer Abuse Policy
* Online Learning Policy
* [Link to policies](https://www.thehavenschool.com/policy-documents-2/)

# Appendix 1: acceptable use agreement (pupils and parents/carers)

|  |
| --- |
| **Acceptable use of the school’s ICT systems and internet: agreement for pupils and parents/carers** |
| **Name of pupil:**  |
| **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 a bring a phone to school, I will hand it into the office each morning. (KS3&4)\*If I bring a personal mobile phone or other personal electronic device into school (6th Form Only)\** 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. |
| **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:** |

\*Delete as appropriate

# Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

|  |
| --- |
| **Acceptable use of the school’s ICT systems and the internet: agreement for staff, governors, volunteers and visitors** |
| **Name of staff member/governor/volunteer/visitor:**  |
| 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. |
| **Signed (staff member/governor/volunteer/visitor):**  | **Date:** |

# Appendix 3: online safety training needs – self-audit for staff

|  |
| --- |
| **Online safety training needs audit** |
| **Name of staff member/volunteer:** | **Date:** |
| What is the name of the person who has lead responsibility for online safety in school? |  |
| What must you do if a pupil approaches you with a concern or issue?  |  |
| Are you familiar with the school’s acceptable use agreement for staff, volunteers, governors and visitors? |  |
| Are you familiar with the school’s acceptable use agreement for pupils and parents?  |  |
| Do you regularly change your password for accessing the school’s ICT systems? |  |
| Are you familiar with the school’s approach to tackling cyber-bullying?  |  |
| Are there any areas of online safety in which you would like training/further training? Please record them here.  |     |