VOYAGE LEARNING CAMPUS

Voyage Learning Campus

ONLINE SAFETY POLICY

This policy has been adopted by the Senior Leadership Team on:	
Date adopted:	9th March 2021
Signed:	
Next review due:	March 2023

Contents

1. Aims

At the Voyage Learning Campus we provide a safe, nurturing, holistic learning environment. This includes our online or virtual environment.

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and Management Committee

- 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 (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 Principals and school staff

- Relationships and sex education

- Searching, screening and confiscation

It also refers to the DfE'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 students' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The Management Committee

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

The Management Committee 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 3)

3.2 The Principal

The Principal 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 and deputy DSL

Details of the school's DSL and deputy DSL are set out in our Child Protection and Safeguarding policy as well as relevant job descriptions.

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 Online Learning Manager and other staff, as necessary, to address any online safety issues or incidents

- Ensuring that any online safety incidents are logged (see appendix 5) 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 Anti Bullying Policy

- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

3.4 The Online Learning Manager

The Online Learning 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 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 termly 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 5) and dealt with appropriately in line with this policy

- Working with the head of the phase, ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Anti Bullying Policy

- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Providing regular reports on online safety in school to the Principal and/or Management Committee

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 3), and ensuring that students follow the school's terms on acceptable use (appendices 1 and 2)

- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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 Anti Bullying policy

  This list is not intended to be exhaustive; staff should also refer to the Staff Code of Conduct and government legislation outlined in section 2.

3.6 Parents/Carers

Parents/Carers are expected to:

- Notify a member of staff or the Principal 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 (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre

- Hot topics - Childnet International

- Parent factsheet - Childnet International

- Healthy relationships – Disrespect Nobody

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 3).

4. Educating students about online safety

Students will be taught about online safety throughout the curriculum. This will include how to:

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

- 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

- The safe use of social media and the internet will also be covered

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website and social media. This policy will also be shared with parents/carers.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the key tutor who will discuss with senior staff, the DSL and/or the Online Learning Manager as appropriate.

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

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.

Procedures for preventing and managing cyber-bullying are outlined in our Anti Bullying policy.

6.2 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 students' 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

  Staff should not make a copy or send themselves any images that fall within procedures outlined in the Child Protection and Safeguarding Policy.

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

7. Acceptable use of the internet in school

All students, parents/carers, staff, volunteers and Management Committee are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). 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 students, staff, volunteers, Management Committee and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Students using mobile devices in school

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

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

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement will be managed by senior staff in the school.

9. Staff using work devices outside school

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 – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring no data is stored on the hard drive – this means if the device is lost or stolen, no one can access the files stored on the hard drive. School files must always be accessed via the school VPN
- Making sure the device locks if left inactive for a period of time, or manually locking the device if leaving it unattended
- Not sharing the device among family or friends
- Keeping anti-virus software up-to-date
- Keeping operating systems up to date – always install the latest updates
- Informing the Online Learning Manager of any issues, particularly relating to the security of their device

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice the Online Learning Manager.

10. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our Relationship and Behaviour policy and Anti bullying 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 policy and Staff Code of Conduct policy. 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 and deputy DSL 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.

Management Committee members 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 5.

This policy will be reviewed every 2 years by the Online Learning Manager.

13. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding policy
- Relationship & Behaviour policy
- Disciplinary policy (staff)
- Data Protection policy and privacy notices
- Complaints Procedure
- ICT and Internet Acceptable Use policy
- Remote Learning policy

Appendix 1: Phase One acceptable use agreement (students and parents/carers/)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS/CARERS

Name of student:

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

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - o I click on a website by mistake
    - o I receive messages from people I don't know
    - o I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

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

Signed (student):	**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 students 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 2: Phase 2 and 3 acceptable use agreement (students and parents/carers/)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS/CARERS

Name of student:

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

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

- Always use the school'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/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- 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
- Log in to the school's network using someone else's details
- 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 and that there will be consequences if I don't follow the rules.

Signed (student):	**Date:**

Parent/carer's 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 students 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: acceptable use agreement (staff, Management Committee, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, MANAGEMENT COMMITTEE,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 (if applicable), I will not: - Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)   - 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, or connect unauthorised hardware or devices to the school's network   - Share my password with others or log in to the school's network using someone else's details   - Take photographs of students without checking with teacher's first   - Share confidential information about the school, its students or staff, or other members of the community   - Access, modify or share data I'm not authorised to access, modify or share   - Promote private businesses, unless that business is directly related to the school

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 and my use of the school's ICT facilities and systems.
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 Online Learning Manager know if a student 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 students in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, Management Committee and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents/carers?	
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?	

Appendix 5: 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**