NEW FOREST CENTRE

Outdoor Learning Centre Online Safety Policy

POLICY No. nfce_hsp_1015

Prepared by Name: Mark Fry

Approved: 07/12/2021

Document Revision No: 1.0

Contents

1. Aims

Our Centre aims to:

- Have robust processes in place to ensure the online safety of students, staff and volunteers
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Centre 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 Head of Centres and school staff
- Relationships and sex education
- 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 students' 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 Directorship

The directorship has overall responsibility for monitoring this policy and holding the Head of Centre 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).

All directors will:

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

3.2 The Head of Centre

The Head of Centre is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the Centre.

3.3 The Designated Safeguarding Lead (DSL)

Details of the Centre's DSL and deputies are set out in our child protection and safeguarding policy as well relevant job descriptions.

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

- Supporting the Head of Centre in ensuring that staff understand this policy and that it is being implemented consistently throughout the Centre
- Working with the Head of Centre, 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 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 Centre behaviour policy
- Updating and delivering staff training on online safety (appendix 4 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 Centre to the Head of Centre and Director of Education 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 students safe from potentially harmful and inappropriate content and contact online while at Centre, including terrorist and extremist material
- Ensuring that the Centre'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 Centre's ICT systems on a monthly 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
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Centre behaviour policy

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 Centre's ICT systems and the internet (appendix 2), and ensuring that students follow the Centre's terms on acceptable use (appendices 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Centre behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Head of Centre of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the Centre's ICT systems and internet (appendices 1)

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

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

3.7 Visitors and Members of the Community

Visitors and members of the community who use the Centre'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 as part of the curriculum:

Students 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

- *By the **end of primary Centre**, students 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 Key Stage 3, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

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

The Centre will use 1:1 and group sessions to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating Parents about Online Safety

The Centre 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 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 Head of Centre and/or the DSL.

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

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 Centre behaviour policy.)

6.2 Preventing and Addressing Cyber-bullying

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

The Centre will actively discuss cyber-bullying with students, 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, Directors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

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

Centre 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. This would always be done in collaboration with placing school or Local Education Authority.

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 Centre 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 Centre discipline), and/or
- Report it to the police

Any searching of students 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 students' electronic devices will be dealt with through the Centre complaints procedure.

7. Acceptable use of the Internet in Centre

All students, parents, staff, volunteers and directors are expected to sign an agreement regarding the acceptable use of the Centre's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the Centre's terms on acceptable use if relevant.

Use of the Centre'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, directors 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 Centre

Students may bring mobile devices into Centre if agreed between the Centre and parents/carers. The device should be handed in to the Centre office for safekeeping during the day. Students are not permitted to use them during:

- Lessons
- Tutor group time

Unless specifically agreed with the Senior Leadership Team/Teacher and student, for example: use within an ICT lesson.

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

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

9. Staff using Work Devices Outside Centre

Staff members using a work device outside The Centre must not install any unauthorised software on the device and must not use the device in any way which would violate the Centre's terms of acceptable use, as set out in appendix 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 Centre. Any USB devices containing data relating to the Centre 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 Centre will respond to Issues of Misuse

Where a student misuses the Centre's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and 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 Centre'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/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The Centre 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 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.

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 year by the Head of Centre. 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
- ICT and internet acceptable use policy

Appendix 1: KS2 and KS3 acceptable use agreement (students and parents/carers)

ACCEPTABLE USE OF THE CENTRE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS	
Name of student:	
I will read and follow the rules in the acceptable use agreement policy **When I use the Centre's ICT systems (like computers) and get onto the internet in Centre I will:** • Always use the Centre'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 Centre'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 Centre:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the Centre, 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 Centre 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 Centre's ICT systems and internet when appropriately supervised by a member of Centre staff. I agree to the conditions set out above for students using the Centre's ICT systems and internet, and for using personal electronic devices in Centre, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

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

ACCEPTABLE USE OF THE CENTRE'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/director/volunteer/visitor:	
When using the Centre's ICT systems and accessing the internet in Centre, or outside Centre 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 Centre'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 Centre's network • Share my password with others or log in to the Centre's network using someone else's details • Take photographs of students without checking with teachers first • Share confidential information about the Centre, 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 Centre	
I will only use the Centre's ICT systems and access the internet in Centre, or outside Centre on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the Centre will monitor the websites I visit and my use of the Centre'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 Centre, and keep all data securely stored in accordance with this policy and the Centre's data protection policy. I will let the designated safeguarding lead (DSL) and ICT 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 Centre's ICT systems and internet responsibly, and ensure that students in my care do so too.	
Signed (staff member/director/volunteer/visitor):	**Date:**

Appendix 3: 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 Centre?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the Centre's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the Centre's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the Centre's ICT systems?	
Are you familiar with the Centre's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	