



**Ocean Academy Poole**  
an Aspirations Academy

## **Online Safety Policy**

<b>Approved By</b>	<b>CEO South Coast</b>
<b>Last Reviewed</b>	January 2024
<b>Next Review</b>	January 2026

# 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
- To understand and support the 4 Cs: content, contact, conduct and commerce

## Content

Content is anything posted online - it might be words or it could be images and video. Children and young people may see **illegal, inappropriate or harmful content** when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

## Contact

Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of **grooming** or exploiting a child or young person for sexual, criminal, financial or other purposes.

## Conduct

Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, **online bullying**. Conduct also includes things like sharing or **receiving nudes and semi-nude images** and viewing or sending pornography.

## Commerce

Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applies to staff.

# 2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education 2023](#), 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](#).

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

# 3. Roles and responsibilities

## 3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Principal 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 Mandy Lancey, supported by the regional safeguarding officer.

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 IT systems and the internet

### **3.2 The Principal**

The Principal and the Online Safety lead are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Principal will ensure there is a member of staff who is responsible for leading online safety across the academy and that they will receive relevant and up to date training to carry out this role.

### **3.3 The Designated Safeguarding Lead**

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

The DSL, alongside the Online Safety lead, take lead responsibility for online safety in school, in particular:

- Ensure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the deputy DSLs, IT manager, Online Safety lead and other staff, as necessary, to address any online safety issues or incidents
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Ensuring that any online safety incidents are logged on MyConcern 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
- 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 IT support**

The IT support 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
- Carrying out regular breach monitoring and alerting staff of any possible breaches
- Ensuring that the school's IT 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 IT systems on a weekly 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 MyConcern 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

### 3.5 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 IT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL and Online Safety lead to ensure that any online safety incidents are logged on MyConcern 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
- Read and adhere to the Acceptable Use policy with regards IT and online platforms and equipment

### 3.6 Parents

Parents 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 IT systems and internet
- Use social media responsibly and monitor their child's use of social media and the internet at home
- 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>

*Parent online safety resources, Childnet International:* <https://www.childnet.com/resources>

*Commonsense Media:* <https://www.common sense media.org/>

*Internet Matters:* <https://www.internetmatters.org/>

*National Online Safety* <https://nationalonlinesafety.com/>

### 3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT 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.

## 4. Educating pupils about online safety

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

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 and what systems the academy uses to filter and monitor (Smoothwall) in letters or other communications home, and in information via our website.

Online safety will also be covered during parents' evenings – handouts will be given to those who attend and posted to those who do not attend.

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 Principal.

The Safer Schools Team will come into school to deliver information to staff, parents and pupils.

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way.

The academy has invested in the National Online Safety platform and has offered parents the opportunity to subscribe to this free of charge.

Parents and carers will be encouraged to support the academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website / Learning Platform and on-line student / pupil records
- Their children's personal devices in the school / academy (where this is allowed)
- Their children's school Google accounts when used outside of the school

## **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.)

Cyber-bullying is also referred to in the schools anti-bullying policy.

### **6.2 Preventing and addressing cyber-bullying**

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

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

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.

Parents will be informed if there has been any inappropriate use of electronic devices.

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

5

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.

### **6.4. Artificial Intelligence (AI)**

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Ocean Academy recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The academy will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the academy.

## **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 IT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use. This can be found on the academy website.

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.

## **8. Pupils using mobile devices in school**

Pupils may bring mobile devices into school, but are not permitted to use them during the school day. They must hand the phone to a member of staff when they come into school and collect it again at the end of the day.

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

## **9. Staff using work devices outside school**

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

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. USB devices containing data relating to the school should not be used if possible and if they do need to be used, **must** be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the IT manager or Online Safety lead.

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 IT 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 IT 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.

6

## **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 (induction training and INSET / staff meetings)

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/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.

Members of the South Coast Regional Board will ensure safeguarding leads have the correct training to fulfill their role.

The Online Safety lead will undergo training in order to fulfill their role.

Ocean Academy has subscribed to the National Online Safety platform and this enables relevant and up to date training for all staff and parents.

Volunteers will receive appropriate training and updates, if applicable. Induction procedures include online safety training.

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 on My Concern.

This policy will be reviewed every 2 years by the Online Safety lead (Mr J lee). At every review, the policy will be shared with the South coast CEO.

Mandy Lancy (Aspirations Safeguarding Lead) audits Ocean Academy's procedures annually in a comprehensive review process. Safeguarding (including online safety) is also a standing item on the South Coast District Board agenda.

## **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
- Anti-bullying policy
- GDPR policy