Educational Diversity

Online Safety Policy

Approved by:	Headteacher	**Date:** Spring 2019
Last reviewed on:	March 2025	
Next review due by:	March 2026	

2. Legislation and Guidance

3. Roles and Responsibilities

4. Educating Pupils about Online Safety

5. Educating Parents about Online Safety

6. Cyber-Bullying

7. Acceptable use of the internet in school

8. Pupils using mobile devices in school

9. Staff using work devices outside school

10. How the school will respond to issues of misuse

11. Training

12. Monitoring arrangements

13. Links with other policies

Appendix 1: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

Appendix 2: Acceptable Use Agreement (staff, management committee, volunteers and visitors)

Appendix 3 Online Safety Training Needs – Self Audit for Staff

Appendix 4: Online Safety Incident Report Log

This policy should be read in conjunction with our Anti-Bullying Policy, our SEND Policy, our Relationships and Behaviour Policy and our Safeguarding Policy.

1. Aims

At Educational Diversity we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and management committee members
- 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
- Cyber-bullying: advice for headteachers and school staff
- 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 Management Committee

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

The Management Committee will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All Management Committee members will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms of acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The Headteacher

Our 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 (DSL) /Deputy Designated Safeguarding Lead (DDSL)

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

The DSL/DDSL take 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 and ICT Teachers and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the school 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 school to the headteacher and/or management committee This list is not intended to be exhaustive.

3.4 Blackpool Council ICT team

Educational Diversity has an SLA with the Blackpool Local Authority who have responsibility 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
- Performing constant security checks and monitoring on the hosted environment. This is via the SIEM, SCCM, VMware monitoring tools, these are all in real time. TNP constantly monitors the network. Patching is completed monthly unless there is an emergency patch and this is done within 3 days. There is also real-time alerting for suspicious behaviour via the Office365 Cloud Security portal.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are shared with the School Business Manager who in turn will add this to the CPOMs system which notifies the DSL.

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 of acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL/DDSL 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 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
- Parents 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 fact sheet - Childnet International

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 of acceptable use (appendix 3).

4. Educating Pupils about Online Safety

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

Pupils in **our Primary Provision** 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

In **Key Stage 3, pupils** 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

Pupils in **Key Stage 4** will be taught:

- The need to follow safe practices outside the ICT room in educational settings. Learners will understand the importance of safe practices when using ICT systems in public, within a working environment and at home.
- To keep access information secure by using passwords.
- To understand the danger of computer viruses and how to minimise risk.
- To recognise and take account of copyright and other constraints on the use of information.
- The nature of the internet and how information (e.g. information on social networking sites) is accessible to a range of individuals.
- To know when it is appropriate / inappropriate to disclose their own personal information.
- To respect other people's personal information when using ICT-based communication.

The safe use of social media and the internet will also be covered in other subjects where relevant. The school will use one to one meetings and parent meetings 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

Educational Diversity 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.

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/DDSL.

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. (Also see 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.

At Educational Diversity we actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class and form tutors will discuss cyber-bullying with their tutor groups.

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, management committee 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).

We share 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, we follow the processes set out in our 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/DDSL 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/DDSL 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
- Contact/Refer to CSC

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 at Educational Diversity

All pupils, parents, staff, volunteers and the Management Committee are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1 & 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, management committee and visitors (where relevant) to ensure they comply with the above. Weekly Prevent Reports are received from **fortianalyzer@blackpool.gov.uk**

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 to school, but these are taken from them on arrival and kept safe until they leave at the end of their day.

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.

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 Local Authority ICT Team on 01253 478787. Work devices must be used solely for work activities.

10. How Educational Diversity Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our cyber bullying policy if that is appropriate or our relationships and 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 code of conduct, computer and network use policy and the disciplinary 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 Headteacher, DSL and all staff will undertake child protection and safeguarding training at a level appropriate to their role and as detailed in the Safeguarding Policy.. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Management Committee members access 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/DDSL logs behaviour and safeguarding issues related to online safety as appropriate .

This policy will be reviewed every 2 years by the DSL/DDSL. At every review, the policy will be shared with the management committee.

13. Links with Other Policies

This online safety policy is linked to our:

- Child Protection and Safeguarding policy
- Relationships and Behaviour policy
- Staff Disciplinary Procedures

- Data Protection Policy and Privacy notices
- Complaints Procedure
- ICT and Internet Acceptable Use Policy

Appendix 1: KS1, KS2, KS3 and KS4 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:

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 (including google and other apps) 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 (pupil):	**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 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:**

Appendix 2: 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/Management Committee Member/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 pupils without checking with teachers first
- Share confidential information about the school, its pupils 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) 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/Management Committee Member/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 pupil 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 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?	