Online Safety Policy

DSL	**Mr Neil Ward**
Last Updated	**August 2023**
Approved by the Governing Body/Board	
Date to Review	**August 2024**

Aims

We aim to:

- Have robust processes in place to ensure the online safety of pupils and staff
  Educate the risk and benefits to being online

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, 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.

Roles and responsibilities

Neil Ward is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead

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

The DSL takes lead responsibility for online safety in particular:

- Supporting staff to understand this policy and that it is being implemented
- Working with staff, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged 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 and the 4ward sports policy
- Updating staff training
- Liaising with other agencies and/or external services if necessary
- Ensuring that any online safety incidents are logged
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with l behaviour policy

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
- Working with the DSL to ensure that any online safety incidents are dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the behaviour policy

Parents

Parents are expected to:

- Notify a member of staff of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use

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/advicecentre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Educating pupils about online safety

Pupils will be taught about online safety

Pupils 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

Cyber-bullying

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.)

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.

All staff, will receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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. All incedents will be reported to the head teacher of the school.

Use of mobile devices (Including phones)

4ward sports allows staff to bring in personal mobile phones. Staff mobile phones can only be accessed in the staffroom for personal use. Staff will need to use phones for access to registers, child records and contact details.

Under no circumstances does the school allow a member of staff to contact a pupil.

Pupils are allowed to bring personal mobile devices/phones to the after school club but they must be handed to a member of staff and kept in a safe and secure place.

At all times the device must be switched onto silent.

4ward sports are not responsible for the loss, damage or theft of any personal mobile device.

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

School Provided Mobile Devices (including phones)

The sending of inappropriate text messages between any member of the school community is not allowed.

Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.

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.

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.

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.

Monitoring arrangements

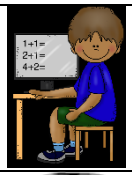
The DSL monitors reports of behaviour and safeguarding issues related to online safety.

This policy will be reviewed by the DSL

4ward sports

Pupil ICT Acceptable Use Agreement

We understand the importance and benefits of using computers to help with children's learning and personal development. However, we also recognise that safeguards need to be in place to ensure children are kept safe at all times.
Please could parents or carers read and sign this agreement with their child

	**I will ask a teacher or suitable adult if I want to use the computers/tablets**
	**I will only use activities that a teacher or suitable adult has told or allowed me to use**
	**I will take care of computers/tablets and other equipment**
	**I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong**
	**I will tell a teacher or suitable adult if I see something that upsets me on the screen**
	**I know that if I break the rules I might not be allowed to use a computer/tablet**

I have read and understand these rules and agree to them.

Child Signature…… Class ……

Parent or Carer Signature…… Date ……..

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF

Name of staff member/volunteer:

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 teacher's 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) and ICT manager (Blue Orange) 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:**