New Direction School

Online Safety and Internet use Policy

Reviewed Date:	Reviewed By:	List of changes	Next Review
August 2021	Luke Collins	● Mobile phones section expanded to include use of mobile phones in school ● Social media appendix added.	August 2022
16th February 2022	Luke Collins	● Reviewed by Luke Collins with some minor grammatical changes made.	January 2023
21st February 2023	Luke Collins	● Reviewed by Luke Collins with no changes made	February 2024

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils and Staff
- 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
- Support children to develop safer online behaviours both in and out of school.
- Safeguard children and young people in the digital world.
- Emphasise learning to understand and use new technologies in a positive way.

The rapid development and accessibility of the internet and new technologies such as personal publishing and social networking means that E-Safety is an ever growing and changing area of interest and concern.

Our E-Safety policy must reflect this by keeping abreast of the vast changes taking place around us. With this in mind, the policy will be reviewed every year.

Our E-Safety policy operates in conjunction with our Behaviour and Child Protection Policies.

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 headteachers and school staff
- Relationships and sex education (RSE)
- 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 pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The Proprietor

The Proprietor has overall responsibility for monitoring this policy and its implementation.

The Proprietor 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 Proprietor 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 Deputy headteachers

The Deputy headteachers are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and deputy 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:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, deputy head 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 through educare courses
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher

This list is not intended to be exhaustive.

3.4 Designated Staff

Designated Staff are 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
- 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
- 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 our Safeguarding reporting software 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.

3.5 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
- Monitoring students online and supervising students on the computers at all times.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use.
- Logging all incidents on Cpoms, alerting and working with the DSL to ensure that the 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 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 within this policy

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 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.

4. Educating pupils about online safety

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

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:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

*By the **end of secondary school**, pupils will know:*

- *Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online*

- *About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online*
- *Not to provide material to others that they would not want shared further and not to share personal material which is sent to them*
- *What to do and where to get support to report material or manage issues online*
- *The impact of viewing harmful content*
- *That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*
- *How information and data is generated, collected, shared and used online*
- *How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours*

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

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website.

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 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. (See also 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.

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 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 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.

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

Any searching of pupils 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 pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

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 and visitors (where relevant) to ensure they comply with the above.

Internet Access – staff must not access or attempt to access any sites that contain any of the following: child abuse, pornography, promoting discrimination of any kind, promoting racial or religious hatred, promoting illegal acts, any other information which may be illegal or offensive to colleagues.

Access to any of the following should be reported to Derbyshire Police, images of child abuse (sometimes incorrectly referred to as child pornography). These images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative, adult material that potentially breaches the Obscene Publication Act; criminally racists material in the UK.

Social Networking – sites are blocked in school.

Staff should fully acquaint themselves with the privacy settings that are available on any social networking profile in order that profiles are not publicly available.

Members of staff should never knowingly become "friends" with students on any social networking site or engage with pupils on internet chat.

Staff should not use social networking sites to comment on school life or issues. See Appendix 1 for more information.

Use of Email – all members of staff should use their professional Gmail address for conducting school business. Students will be allocated Gmail school accounts to log on to use the gsuite facilities. Any student work or online school communication with students must always happen through the school gmail accounts. Personal emails must never be used.

Passwords – staff should keep passwords private. Passwords are confidential and individualised to each person. On no account should a member of staff allow a student to use a staff login.

Data Protection – where a member of staff has to take home sensitive or confidential information sufficient safeguards should be in place to prevent loss or misuse. USB memory sticks should be encrypted, as they can be easily misplaced. Laptops should be protected with passwords.

Personal Use – staff are not permitted to use ICT equipment for personal use.

Images and Videos – staff and pupils should not upload onto any Internet site, images or videos of themselves or other staff or pupils.

8. Mobile Phones in school

At New Direction we recognise that mobile phones, including smart phones, are an important part of everyday life for our pupils, parents and staff, as well as the wider school community.

We aim to:

- Promote, and set an example for, safe and responsible phone use
- Set clear guidelines for the use of mobile phones for pupils, staff, parents and volunteers
- Support the school’s other policies, especially those related to child protection and behaviour

Some of the challenges posed by mobile phones in school include:

- Risks to child protection
- Data protection issues
- Potential for lesson disruption
- Risk of theft, loss, or damage
- Appropriate use of technology in the classroom

Staff

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, or send texts, during school hours. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present.

There may be circumstances in which it’s appropriate for a member of staff to have use of their phone during contact time. For instance:

- For emergency contact by their child, or their child’s school
- In the case of acutely ill dependents or family members

The headteacher will decide on a case-by-basis whether to allow for special arrangements.

If special arrangements are not deemed necessary, school staff can use the school office number 01246 810456 as a point of emergency contact.

Staff must refrain from giving their personal contact details to parents or pupils, including connecting through social media and messaging apps. If contact is needed with parents from a personal phone then you must ensure your number is blocked to prevent parents from obtaining your number

Staff must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents or pupils.

Staff must not use their mobile phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil. If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but aren't limited to:

- Emergency evacuations
- Supervising off-site trips
- Supervising residential visits

In these circumstances, staff will:

- Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct
- Not use their phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil
- Refrain from using their phones to contact parents. If necessary, contact must be made via the school office

Students

Students may NOT bring mobile devices into school.

Students will be searched and scanned on arrival and expected to hand in their mobile phone.

- Phones will be confiscated (Schools are permitted to confiscate phones from pupils under sections 91 and 94 of the Education and Inspections Act 2006)
- They are kept locked away by staff and only handed back to the student when they are going home.
- Any student breaking this policy will be sanctioned as detailed in the behaviour policy.

Confiscated phones will be stored in the School Library in a locked Cabinet.

Lost phones should be returned to Luke Collins/Hannah Oliver. The school will then attempt to contact the owner.

Parents and visitors

Parents, visitors and volunteers (including contractors) must adhere to this policy as it relates to staff if they are on the school site during the school day.

This means:

- Not taking pictures or recordings of pupils, unless it's a public event (such as a school fair), or of their own child
- Using any photographs or recordings for personal use only, and not posting on social media without consent
- Not using phones in lessons, or when working with pupils

Parents, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school.

Parents or volunteers supervising school trips or residential visits must not:

- Use their phone to make contact with other parents

- Take photos or recordings of pupils, their work, or anything else which could identify a pupil

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 all work for New Direction is saved onto their google drive and not kept on their hard drive/ external hard drive.
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use within this policy.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Luke Collins

10. How the school will 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 policies on behaviour. 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 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.

11. Staff Training

All new staff members will receive training, through educare, 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 and staff meetings).

The DSL and deputy 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.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring and review

12.1 Monitoring

The Proprietor will regularly monitor the operation of this policy and its procedures.

This policy will be reviewed annually by the Proprietor and key staff.

Appendix 1 – Social Media Use

Personal use of social media

- School staff will not invite, accept or engage in communications with parents or children from the school community in any personal social medial whilst employed at New Direction.
- Any communication received from children on any personal social media sites must be reported to the designated Child Protection Officer (The Proprietor).
- If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.
- Members of staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.
- All email communication between staff and members of the school community on school business must be made from an official school email account.
- Staff should not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Head teacher.
- Staff are advised to avoid posts or comments that refer to specific, individual matters related to the school and members of its community on any social media accounts.
- Staff are also advised to consider the reputation of the school in any posts or comments related to the school on any social media accounts.
- Staff should not accept any current pupil of any age or any ex-pupil of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.