Meadows School

London Road, Southborough, TN4 0RJ
enquiries@meadowsschool.org.uk

Online Safety

1. Introduction:

Meadows School is committed to Barnardo's Basis and Values, which provides the framework within which we can engage in giving young people a better start in life.

- We recognise our moral and statutory responsibility to safeguard and promote the welfare of all pupils.
- We endeavour to provide a safe and welcoming environment where children are respected and valued.
- We are alert to the signs of abuse and neglect and follow our procedures to ensure that children receive effective support, protection and justice.
- We understand that as a Special School we are working with some of the most vulnerable young people in the UK and therefore have a duty to ensure stringent procedures and training must be in place and available to all staff.

The procedures contained in this policy apply to all staff, volunteers and governors and are consistent with those of the Kent Safeguarding Children Board (KSCB).

2. Aims:

The school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, visitors 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, including mobile and smart technology (which we refer to as 'mobile devices')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

3. Legislation & 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 Principals and school staff
- Relationships and sex education
- 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.

4.	Roles & Responsibilities:

The Principal
The Principal 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 school's DSL and deputies 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 Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- 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
- 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 Principal and/or governing board

The Data Manager
The Data Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept 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
- Ensuring systems are compliant with Barnardo's IT Code of Conduct
- Conducting a full security check and monitoring the school's ICT systems on a termly 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 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

4.	Roles & Responsibilities Continued:

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 and Barnardo's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- 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 school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

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 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 resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

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

5.	Educating Students:	Pupils will be taught about online safety as part of the curriculum: **All** schools have to teach: › Relationships education and health education in primary schools › Relationships and sex education and health education in secondary schools 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 By the **end of primary school**, pupils 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 › What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context) › 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**, 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

5.	Educating Students Continued:	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 › How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online) The safe use of social media and the internet will also be covered in other subjects where relevant.

6.	Supporting Parent Understanding:	• The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). • If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL. • Concerns or queries about this policy can be raised with the Principal.

7. 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.

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. 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, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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.

8. 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*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

Meadows School uses Smoothwall Filtering and Smoothwall Monitoring to support this process – parents wishing to have more information on these pieces of software should speak with the Data Manager ion the first instance.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

9. Acceptable Use of the Internet:

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements.

10.	Pupils Using their own Devices in School:	Pupils may bring mobile devices into school, but are not permitted to use them during: › Lessons › Tutor group time › Clubs before or after school, or any other activities organised by the school Any use of mobile devices in school by pupils must be in line with the acceptable use agreement. 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.
11.	Staff Using Work Devices Outside of 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 their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device › Making sure the device locks if left inactive for a period of time › Not sharing the device among family or friends › 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 or Barnardo's terms of acceptable use. 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 the IT team.
12.	Responding to Misuse:	Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and safeguarding. 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.

13. 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).
By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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.

In line with DfE guidance, all staff will complete the National Cyber Security Centre's 'Cyber Security Training for School Staff'

14. Monitoring & Review:

The DSL logs behaviour and safeguarding issues related to online safety.
This policy will be reviewed every year by the Data Manager. At every review, the policy will be approved by the Chair of Governors and ADCS then republished on the school website.

15.	Additional Information
Copies of this policy may be obtained from:	• Share Point • www.meadowsschool.org.uk
This policy links with the following policies & Documents	› Child protection and safeguarding policy › Behaviour policy › Staff disciplinary procedures › Data protection policy and privacy notices › Complaints procedure
Relevant statutory guidance, circulars, legislation & other sources of information are:	Keeping Children safe in Education - 2021
The lead member of staff is:	Lizzie Harlock