



MOORFIELD  
SCHOOL

## E-SAFETY POLICY



This policy is applicable to all electronic devices that can access the internet.

(This Policy is also applicable to the EYFS)

# E-SAFETY POLICY

## Purpose

It is important that children learn how to be safe when they are using new technologies. Whilst blocking and banning is part of our policy, we believe a more sustainable approach is required. We will equip the children with the skills and knowledge they need to use the Internet safely and responsibly, managing the risks wherever and whenever they go online; to promote safe and responsible behaviours in using technology both at school, in the home and beyond. The computers are provided and maintained for the benefit of all children, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Pupils are responsible for good behaviour on the Internet just as they are in a classroom or around school.

## Safety online for pupils at school

On-line safety is taught through the computing curriculum and lessons dedicated to this are repeated at the beginning of every term. Pupils also learn about on-line safety through events such as NSPCC workshops in school, Anti-bullying Week and through the PSHE curriculum. On-line safety, including issues around the Prevent Duty, are also taught through workshops and lessons provided by the Bradford District Cyber Team with West Yorkshire Police.

The policy pays due regard to KCSIE 2023, in particular the reference to the four areas of risk, content, contact, conduct and commerce, as categorized in the KCSIE 2023.

## Filtering and Monitoring

The Technical Staff (DataCable), Designated Safeguarding Lead, Senior Leadership Team and the network manager are responsible for ensuring the technical infrastructure is secure and is not open to misuse or malicious attack. The leadership team and DSL receive updates from the technical team about software changes which may affect or improve filtering. DataCable has installed web filtering software to ensure the protection of its pupils whilst accessing the internet. Currently, the school has the Schools Broadband filtering software in place. This is called NetSweeper and meets all the requirements for KCSiE 2023.

Other security measures include:

- Separate levels of filtering, office, pupils and staff
- Each log-in to a Windows device is tracked online to the filtering system
- Log created which shows which banned internet sites have had an attempted access
- Logs can be automatically generated and emailed to Designated Safeguarding Lead or person responsible for on-line safety
- Meets all government guidelines for Prevent Duty and Keeping Children Safe in Education

Further information and an overview can be found at:

<https://www.schoolsbroadband.co.uk/e-safety-filtering-and-security>

For monitoring purposes, the software package, 'classroom.cloud' is installed on all machines and this meets all the requirements of KCSiE 2023. This is a software package that's installed on all machines. The software works by monitoring the user and anything they typed, searched or used on that particular machine. If a

concern arises, it is recorded and rated accordingly and an email alert is triggered and sent to the safeguarding team.

It is recognised that no software is infallible.

## Acceptable use

In order to keep children safe online at Moorfield the following rules apply:

### Equipment

- Do not install, attempt to install or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.).
- Do not eat or drink near computer equipment.

### Security and privacy

- Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet your home address, your telephone number, any details about Moorfield, or send them your picture.
- Do not use the computers in a way that harasses, harms, offends or insults others.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Computer storage areas will be treated like school desks. Staff may review files and communications to ensure that users are using the system responsibly.

### Internet

- The Internet should only be used for study or for school authorised/supervised activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
  - Respect the work and ownership rights of people outside the school, as well as other pupils or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the Internet. This takes up valuable resources which could be used by others to benefit their studies.
- Never arrange to meet anyone via the Internet. People you contact online are not always who they seem.

### Electronic communication (Email, text, posts)

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed.
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which could destroy information and software on the computers.
- The sending or receiving of electronic messages containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content.
- Always report such messages to a member of staff.

## Enforcement

This document is to be read carefully by all parents and children. If any child violates these provisions, access to the Internet will be denied and disciplinary action may be taken in accordance with the school *Behaviour and Discipline Policy*. Where appropriate, the police may be involved, or other legal action taken.

The following procedures will be abided by when necessary:

Discovery of inappropriate websites by a member of staff or pupil should be reported immediately to the network manager who will report any incident to the school's network service provider. Illegal material within the schools network is a very serious situation and must always be reported to the police. Any incident that involves deliberate inappropriate adult access to illegal material on Moorfield School premises will be dealt with in accordance with the schools *Staff Code of Conduct* and in conjunction with the police and Child Exploitation and Online Protection (CEOP).

Action in the event of illegal material:

- Seek immediate advice from the network manager who will consult with the Head and the police
- Prevent any further access to the device / network location until the correct advice is gained.
- Unless absolutely necessary, DO NOT remove the power from a working device and under no circumstances start a device if it is already switched off.
- Consider if it is necessary to prevent promote access to the device / network location.
- If it is believed a member of staff or pupil has left the site could remove or damage evidence on the device remotely, unplug only the network cable from the back of the device to prevent this access from occurring.
- If the device is already turned off and is no longer realistically possible to prevent further physical access (i.e. due to lack of supervision, high levels of access or an occupied location) disconnect the power at the base unit (not the wall) and remove the device. Store this device securely in a location where no one else can gain access to it and make a note of the date, time and name of the individual who performed this action.

## Safety online for pupils at home – guidance for parents

Protecting children in the online world means thinking beyond the school environment with the advance of internet technology pupils increasingly will have access to personal devices not covered by school's network protection and therefore the emphasis should be on educating all users as to the risks involved and their obligation to act responsibly whilst online.

On-line safety includes awareness of radicalization and the Prevent Duty, grooming and abuse.

## Guidance for Parents

Parents sign our Acceptable Use Agreement with their children at the start of each school year. Parents receive guidance emphasising the importance of E-Safety at the annual parent information evening in September, along with information about the filtering and monitoring systems used in school.

Parent Handbook includes a 'Code of Conduct' for parents which includes information about the use of all mobile devices within school, including all devices which can record images.

Parents are invited to a workshop led by Bradford District Cyber Team to raise awareness of issues in child protection on-line.

Parents must be aware that cyber-bullying is more likely to take place on electronic devices used at home.

## Cyberbullying

This policy applies to all pupils and should be read in conjunction with

*Anti-Bullying Policy, The Safeguarding and Child Protection Policy, and the Behaviour Policy.*

All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or a worrying issue to any member of staff.

## Introduction and Definition

Cyber bullying Cyber bullying can be defined as 'the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, to deliberately upset someone else'. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages, the size of the audience, perceived anonymity, and even the profile of the person doing the bullying and their target.

Cyber Bullying is a form of bullying, although there are some particular features which set it alone from bullying.

The key differences are: -

- Impact – The scale and scope of cyber bullying can be greater than other types of bullying
- Targets and Perpetrators – The people involved may have a different profile to traditional bullies and their targets.
- Location – the 24/7 and anyplace nature of cyber bullying
- Anonymity – The person being bullied will not always know who is attacking them.
- Motivation – Some pupils may not be aware that what they are doing is bullying
- Evidence – unlike other forms of bullying the target of the bullying will have evidence of its occurrence.

## Procedures to help prevent cyber bullying

As with all aspects of pastoral care, education lies at the heart of our approach. Issues associated with the appropriate use of ICT are discussed both inside and outside the classroom. All pupils follow a structured programme of ICT where pupils are instructed on the responsible use of technology. Each time a pupil logs on to the school network advice is given with regard to the safe usage of email and the internet. Work in ICT is supplemented by the PSHE program. Where incidents of cyber bullying do occur, they are monitored and recorded in the same way as all other forms of bullying.

## Support for those being bullied

Cyber bullying is a particularly pernicious aspect of bullying and is recognised as posing significant risk to the welfare of children. Current research into the extent of cyber bullying indicates that it is a feature of many young people's lives. Cyber bullying can have a seriously detrimental impact on a victim for a number of reasons.

- The sense of invasion of an individual's home and personal space.
- The anonymity (at least initially) of the bully.
- The difficulty in controlling electronically circulated messages.
- The ability to broadcast upsetting messages and images to a potentially huge audience.
- The opportunity for others to become involved in the bullying activity.

## Support for the Bully

- It is important for the bully to be aware of the impact of their actions.
- The perpetrator will need to be supported in trying to understand the need to change their attitude and behaviour.
- It is important to recognise that the bully may need emotional support.
- The bully should be involved in all stages of the process including filling in of initial reports, meeting with the child who is being bullied (where deemed appropriate by the mediator) and follow up meetings

## Examples of Cyber Bullying may include

- Threats and intimidating messages sent via computers or mobile phones.
- Cyber-stalking – repeatedly sending unwanted texts or instant messages.
- Pupils who set up website pages and invite others to post derogatory comments about a pupil.
- Pupils who film fights or assaults and circulate them via mobile phones.
- Pupils insulting or making derogatory or threatening statements or statements of a sexual or racial nature via electronic devices.
- Pupils posting fake and/or obscene photographs of the victim on a social networking site.

## Responding to cyber bullying and records

The guiding principles and practices outlined in The Anti-Bullying Policy will underpin our approach when responding to any and all forms of bullying. In addition to this there may be a need to report the incident to the Designated Person for Safeguarding / Child Protection officer, or Head Tina Herbert.

Please refer to *Anti-Bullying Policy* for procedures and sanctions.

## Use of mobile phones, cameras and other electronic devices

### Pupils

Pupils at Moorfield are not allowed to bring mobile phones, smart watches, fit-bits or any mobile devices to school. The only exception is if children, who walk to school or come on the train, may need a mobile telephone for personal security.

The phone is the pupil's responsibility and parents must inform the school in writing that the child has a mobile phone in their possession for the journey.

The phone must be handed in at the school office on their arrival at school where it will be locked away.

It is the pupil's responsibility to retrieve it at the end of the school day.

Kindles may be used for reading purposes only at the discretion of the classroom teacher and Head. They must be handed in to the teacher in the classroom at the start of the day, retrieved for reading use and handed back. Should a pupil misuse their kindle, they will no longer be allowed to bring this device to school.

Advice against using mobile devices in an inappropriate way with targeted messages, photographs, social media etc. will be covered in PSHE lessons and on-line safety workshops run by PC Danny Mynott.

### Parents

**The school has a legal obligation to protect children whilst in the school's care.**

Parents/visitors are not to use their mobile devices while on school premises in the company of the children.

Parents are allowed to take photos during a school performance but must not upload any photos or videos to any social media platform. Parents sign an agreement to that effect.

#### Staff

Mobile phones belonging to staff must be stored out of sight of children and kept on silent

Mobile phones are not to be used in the classrooms during lesson times, in Breakfast Club or After-School Care either for receiving or sending personal texts, emails or calls. Mobile phones may only be used at break times if no children are present. (Families of staff members can contact the school via the office for any urgent messages.) Mobile phones are not to be used for the taking of photographs.

Always use the school camera.

Designated school mobile phones are available for trips, bus runs, after school care, holiday club, lunch duties etc.

Staff must not use their personal email to contact parents.

Staff mobile devices kept in school must be locked and password protected.

Staff must lock their computers at all times when not using their computers.

Children are not to use staff log in on the computer.

#### TAKING, STORING AND USING IMAGES OF CHILDREN

At Moorfield School, we are an open and inclusive community that is very proud of the achievements of all of our pupils in their academic, artistic and sporting endeavours. We celebrate our diversity and give our visitors a warm welcome.

We particularly welcome parents to our concerts, plays and sporting events, as well as to more formal occasions during the school year. The School walls are decorated with examples of pupils' work, team photographs and photographs of trips and expeditions in which our pupils have participated.

#### THE APPLICATION OF DATA PROTECTION LAWS TO TAKING, USING AND STORING IMAGES OF CHILDREN

Parents who accept a place for their child at Moorfield School are invited to agree to the School using photographs of their child and information relating to their achievements for promotional purposes, which may be published in the prospectus or on the web site, as well as displayed within the premises, and in bulletins sent to the School community. The consent form that we use for this purpose is attached at Annex A. (Full details of the School's Data Protection Policy is available on request). This form is sent to parents to be signed at the start of each academic year.

#### USE OF IMAGES: DISPLAYS ETC

We will only use images of our pupils for the following purposes:

- internal displays (including clips of moving images) on digital and conventional notice boards within the School premises,
- communications with the School community (parents, pupils, staff, Governors and alumni); and
- marketing the School both digitally by website, by prospectus, by displays at educational fairs and other marketing functions or boards, and by other means, such as PR.

#### IMAGES THAT WE USE IN DISPLAYS AND ON OUR WEBSITE

The images that we use for displays and communications purposes never identify an individual pupil, unless parents have given specific permission for this to happen, or it pertains to one particular child. Instead, they name

the event, the term and year that the photograph was taken. We only use images of School activities, such as plays, concerts, sporting fixtures, prize-giving, School trips etc in their proper context. We never use any image that might embarrass or humiliate a pupil. Pupils are always properly supervised when professional photographers visit the School. Parents are given the opportunity to purchase copies of these photographs.

#### STORAGE AND REVIEW

We have a procedure in place for regularly checking and updating our website continually, when expired material is deleted.

#### MEDIA COVERAGE

Parents fill in a form at the start of each year in which they give or withdraw permission for their child's photographs to be taken for the press. We will make every effort to ensure that children whose parents or guardians have refused permission for images of their children to be used are not included in any photographs.

We will complain to the Press Complaints Council (PCC) if the media fails to follow the appropriate code of practice for the protection of young people, including the children of celebrities.

#### STAFF INDUCTION

All new teaching and office staff are given guidance on the School's policy on taking, using and storing images of children. New staff are required to sign that they have read and understood the E-safety policy and sign an Acceptable Use Agreement.

*Drafted by:*

*The Head and Network Manager*

*Date:*

*October 2023*

*Next Review Date:*

*October 2024*





## Moorfield School – ICT Pupil and Parent Agreement

All pupils use computer facilities including Internet access as an essential part of learning, as requires by the National Curriculum. Both pupils and their parents are asked to sign below to show that our Computing Safety rules have been understood and agreed.

### **Pupil Agreement:**

- I will ask permission before using the internet.
- I will immediately tell an adult, and turn off my monitor, if I see any webpage I am uncomfortable with.
- I will only e-mail people an adult has approved and write to them in a polite and friendly manner.
- I will never give out personal information or passwords.
- I will not open e-mails sent by anyone I don't know.
- I will not use chat rooms or social networking sites unless a specific use is approved.
- I will not bring in computer games or files from home unless asked by a teacher.
- I will not bring in an electronic device without prior permission from the Headmistress and the class teacher.
- I understand that the use of a kindle is for reading purposes only.
- I understand that if I misuse my electronic device (e.g. Kindle), I will never be allowed to bring it to school again.
- I will use ICT equipment in a safe and responsible way.
- I understand that the school can check my computer files and the Internet sites I visit.
- I understand that cyberbullying has serious consequences at home and in school.

### **Pupil Declaration:**

My name is (print): \_\_\_\_\_ Signature: \_\_\_\_\_

### **Parent / Guardian Agreement:**

- I understand the school's legal obligation to protect children whilst in its care.
- I agree not to use my mobile phone or any other electronic device while on school premises in the company of the children.
- I agree not to take photographs or videos of school activities with any device.
- I understand that I need to take responsibility for and be knowledgeable about my child's use of the internet at home.
- I understand the risks associated with social media when uploading pictures of children.

Parent / Guardian of : \_\_\_\_\_ Form: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_