MOOR PARK PRIMARY SCHOOL AND NURSERY

ONLINE SAFETY POLICY

September 2024

Part of SYNERGY EDUCATION TRUST

Policy	Online Safety Policy
Blackpool Council model policy	None available *Blackpool procedures and guidance followed*
Reviewed by	Helen Jefferson
Date	September 2024
Approval level	Headteacher
Adopted	04/09/2024
Next review due	September 2025

The importance of online access

Internet access at Moor Park is a necessary tool for staff and students. It will help to raise educational standards, to support the professional work of the staff and to enhance the school's management information and business administration systems.

The benefits of having access

The benefits to be gained through the appropriate use of the Internet are:

- Access to world-wide educational resources including museums and art galleries
- Inclusion in government initiatives
- Exchanges with other schools world-wide
- Discussion with experts in many fields for pupils and staff
- Staff professional development through access to educational materials and good curriculum practice
- Communication with the advisory and support services, professional associations and colleagues
- Improved access to technical support
- Exchange of curriculum and administration data with the LA and DfE
- Promote our school and our learning through our website, blogs and twitter feed
- Internet use enhances planning and assessment procedures across the curriculum.

Providing effective learning through the internet

Teachers, parents and pupils need to develop good practice in using the Internet as a tool for teaching and learning. At Moor Park, Internet access will be planned to enrich and extend learning activities. Staff will select sites, which will support the learning outcomes planned for the pupil's age and maturity, and approved sites will be book marked. Staff will model safe use of the Internet at every opportunity, in line with our Online Safety curriculum.

Assessing content

Teachers will review all material found on the Internet before sharing it with pupils. The teacher/support staff will supervise pupils and take reasonable precautions to ensuring that pupils access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal. Therefore the use of computer systems without the permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.

Any apps being used in a classroom setting must also have been reviewed before allowing access to the children. All apps on mobile devices are Installed by the school technicians (Comptech ITS) and are therefore verified before Installation.

Managing e-mail

Children
All children have access to a school email address provided by our SLA support Comptech ITS and hosted with Microsoft 365. This will be used to access the online classrooms through Microsoft Teams. Email skills are also taught as part of the Computing curriculum in KS2

Staff
All staff have their own e-mail account provided by our SLA support Comptech ITS. E-mail must only be used in school for educational and professional purposes and should not be considered private.

Managing Apps
Apps are becoming increasingly useful in the classroom environment for research and curriculum purposes.

Apps should be reviewed by an adult before installation and will be managed using software which is managed by technician (Comptech ITS).

Moor Park's web pages, Facebook page, Twitter feed and YouTube content.

A Moor Park web site has been created to promote the school. It will be the responsibility of the SLT and admin team to ensure that the web site reflects the school's ethos and that information is accurate and well presented. As the school's web site can be accessed by anyone on the Internet the following rules must be adhered to ensuring the security of both staff and pupils:

- The point of contact on the web site will be the school name and address; individual e-mail addresses and home information will not be published
- Full names will not be used anywhere on the web site
- All parents have completed permission slips allowing their child to be on the website. Each teacher, the school office and the Leadership Team have a list of children **not** allowed to feature in photos & videos.

Authorising access to the internet

Internet access is a necessary part of the statutory curriculum. The majority of the access to the Internet will be by teacher or adult demonstration. However there may be situations when children have supervised access to specific approved on-line materials. All staff with access to the Internet will be asked to sign the Staff Code of Conduct which contains expectations for acceptable use of the internet by staff. The Staff Code of Conduct is read by all staff at the beginning of their employment at the school and beginning of each academic year.
A child friendly search engine "Swiggle" is used by pupils to access the internet.

Online safety curriculum

Online Safety is ongoing and is 'drip fed' into the children's learning at every opportunity to encourage the children to stay safe online. In addition to this ongoing skills approach, the school takes part in the Annual National Online Safety week in February. During this week, teachers deliver a directed, focussed Online Safety curriculum which is progressive across all year groups. The Computing lead also works closely with the PSHE lead and a full half term of PSHE/Online safety lessons is delivered in the Spring term.

Informing Parents

A careful balance between informing and alarming parents about Internet use will be maintained. Parents will be informed that pupils will be provided with supervised Internet access.

If we are informed that children have accessed inappropriate data at school, or posted something in applications, parents are informed and records are kept by school on the Safeguarding system which is monitored by the SLT, DSL and family worker. This team work with the Computing lead if more information/advice is required in this area.

Cyberbullying

Cyberbullying can be defined as "Cyberbullying is bullying that takes place using technology." (DfE 2017) and Childnet say "Bullying is purposeful, repeated behaviour designed to cause physical and emotional distress. Cyberbullying (or online bullying) is bullying using technologies, particularly over the internet or via mobile and gaming networks."

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively.

When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular 'Preventing and tackling bullying' (DfE 2017) says schools should "develop strategies to prevent bullying occurring in the first place." "Schools which excel at tackling bullying have created an ethos of good

behaviour where pupils treat one another and the school staff with respect because they know that this is the right way to behave."

These measures are part of the school's behaviour policy which must be communicated to all pupils, school staff and parents gives headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Where bullying outside school (such as online or via text or social media) is reported to the school, it should be investigated and acted on appropriately. Staff seek guidance from SLT and DSL if this occurs and all Incidents are recorded using the Safeguard software. Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed they should seek assistance from the police.

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

- There are clear procedures in place to support anyone in the school community affected by cyberbullying.

- All incidents of cyberbullying reported to the school will be recorded using Safeguard software

- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

- Sanctions for those involved in cyberbullying may include:

    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.

- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

Filtering and Monitoring

Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, school has systems in place to limit children's exposure to risks from the school's Internet and IT system. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

An active and well managed filtering system is an important part of providing a safe environment for pupils to learn and limiting children's exposure to the 4 categories of risk

- Content – being exposed to illegal, harmful content such as pornography, racism, self harm, radicalisation and extremism
- Contact – being subjected to harmful contact with other users such as adults posing as children or young adults with the intention to groom or exploit for sexual, criminal or financial purposes
- Conduct – personal online behaviour which increases the likelihood of harm such as sending or receiving explicit messages or photographs
- Commerce – exposure to risks such as online gambling, inappropriate advertising, phishing and financial scams.

No filtering system can be 100% effective. An effective filtering system needs to block internet access to harmful sites and inappropriate content. It should not:

- unreasonably impact teaching and learning or school administration
- restrict students from learning how to assess and manage risk themselves

The leadership team and relevant staff have an awareness and understanding of the provisions in place and know how to escalate concerns when identified.

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs

Monitoring

Monitoring user activity on school and college devices is an important part of providing a safe environment for children and staff.

Monitoring will be used to review user activity on school devices. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

Evidencing

When an incident occurs, staff make the DSL, family worker and SLT (where appropriate) aware of the situation. All incidents and Cyberbullying are recorded on the schools Safeguarding software and dealt with accordingly.

Staff are updated regularly of any changes to Online Safety.