Moulton Chapel Primary School
01406 380440
enquiries@moultonchapel.lincs.sch.uk

E-Safety Policy

Aims

Our school is committed to creating a safe and positive online environment for everyone. We achieve this by:

- ***Protecting:*** *Actively promoting and safeguarding the online safety of our pupils, staff, volunteers, and governors.*
- ***Educating:*** *Equipping all members of our school family with the knowledge and skills to navigate the digital world safely and responsibly.*
- ***Empowering:*** *Foster a culture of open communication and reporting, enabling early intervention and resolution of any online safety concerns.*

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users *– refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.*

Parents *– any adult with a legal responsibility for the child/young person outside the school e.g. parents, guardian, carer.*

School *– any school business or activity conducted on or on behalf of the school site, e.g. visits, conferences, school trips.*

Wider school community *– pupils, all staff, governing body, parents.*

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*
- *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 cyberbullying 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 requirements.

Roles and Responsibilities

Governing Body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing body 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).

There is a governor who is responsible for and oversees E Safety

All governors will:

- *Ensure that they have read and understand this policy*
- *Agree and adhere to the terms on acceptable use of the school's IT systems and the internet*

Ratified by Governors: December 2024
Next review: Term 2 2027

Moulton Chapel Primary School
01406 380440
enquiries@moultonchapel.lincs.sch.uk

Headteacher & E-safety Officer

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school but may delegate tasks relating to e-safety to other members of staff.

The Headteacher will:

- *Ensure training throughout the school on e-safety is given and is up to date and appropriate to the recipient.*
- *All e-safety incidents are dealt with promptly and appropriately*
- *Staff have read and understood this policy*
- *Ensuring that any incidents of cyber-bullying are logged and dealt with*
- *appropriately in line with the school behaviour policy*
- *Engage with parents and the wider school community on e-safety matters at school and /or at home*
- *Liaise with the Local Authority or IT technical support and other agencies as required*
- *Have responsibility for the e-safety incident log; and ensure staff know how to report an incident*
- *Work with IT technical support to ensure all technical e-safety measures are in school e.g internet filtering and monitoring of software*

IT technical Support Staff

At Moulton Chapel Primary School we buy in technical support from ARK IT Solutions.

Technical support staff are responsible for ensuring that:

- *The IT infrastructure is secure, this will include a minimum:*
  - *Anti-virus is fit for purpose, up to date and applied to all capable devices.*
  - *Windows updates are regularly monitored, and devices updated as appropriate*
  - *Any e-safety technical solutions such as Internet filtering and monitoring are operating correctly*
  - *Filtering levels are applied appropriately and according to the age of the user*
  - *Passwords are applied correctly to all users regardless of age.*

All staff

Staff are to ensure:

- *All details within this policy are understood. If not, this should be brought to the attention of the Headteacher*
- *Any e-safety incident is reported to the Headteacher, and an incident report log completed (Appendix 1)*
- *Ensuring that any incidents of cyber-bullying are dealt with appropriately in line*
- *with the school behaviour policy.*
- *They have an up-to-date awareness of e-safety matters and this policy*
- *They have read, understood and signed the Acceptable User policy*
- *Online safety issues are embedded in all aspects of the curriculum and other activities*
- *Pupils have a good understanding of what is acceptable use of technology*
- *They monitor the technologies being used in lessons and other school activities and implement current policies to those devices*
- *In lessons where the internet is being used sites have been checked for suitability of use and processes are in place for dealing with any unsuitable material that is found in internet searches.*

All pupils

The boundaries of the using IT equipment and service in this school are given in the Acceptable User policy; any deviation or misuse of IT equipment or services will be dealt with in accordance with our behaviour policy.

Ratified by Governors: December 2024
Next review: Term 2 2027

E-safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly, pupils will be made fully aware how they can report areas of concern whilst at school and outside the school.

Pupils are responsible for:

- *Using technology in accordance with the Acceptable User Policy*
- *Having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations appropriate to their age.*
- *Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.*
- *Know and understand policies on the use of mobile phones and digital cameras in school, taking and use of images and on cyber-bullying.*
- *Understand the importance of adopting good online safety practices when using digital technology inside and outside of school.*

Parents and carers

Parents play an important role in the development of their children as such the school will ensure parents have information on how they can support in keeping their child safe online. We will provide communications through guidance videos, emails, newsletters, links on our school website that help with this.

Parents must also understand that school needs to have rules in place to ensure that their child/ren can be properly safeguarded. As such parents will sign the Pupil Acceptable Use agreement to show their support for this aspect of school life.

Educating pupils about online safety

Pupils will be taught about Online Safety as part of the Curriculum

In Key Stage 1, pupils will be taught to:

- *Use technology safely and respectfully, keeping personal information private.*
- *Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.*

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*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

Curriculum Content - Implementation

- *The school believes it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within the curriculum and the school continually looks for new opportunities to promote e-safety.*

- *The school provides opportunities within a range of curriculum areas to teach about e-safety including, but not limited to, Computing and SMSC. Throughout the curriculum, students learn about internet safety and are offered advice on how to stay safe online.*
- *Pupils are made aware of the dangers when using the internet such as data protection, intellectual property and on-line gaming which may limit what they want to do but also serves to protect them.*
- *Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.*
- *Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying.*
- *Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.*
- *Pupils are taught to critically evaluate materials and learn good searching skills through cross-curricular teacher models, discussions and via the IT.*

Technology

The use of technology has become a significant component of many safeguarding issues. Children exploitation; radicalisation; sexual predation; cyberbullying: technology often provides a platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- *Content: being exposed to illegal, inappropriate, or harmful material.*
- *Contact: being subjected to harmful online interaction with other users; and*
- *Conduct: personal online behaviour that increases the likelihood of, or causes, harm.*

Filters and monitoring

As a school we recognise the importance of doing all that we reasonably can to limit children's exposure to the above risks from our IT system. As part of this process, the governing body ensures the school has appropriate filters and monitoring systems in place through our IT provider, currently ARK IT.

The governing body recognises that whilst filtering and monitoring are an important part of the online safety picture for schools to consider, it is only one part. They consider a whole school approach to online safety which includes use of mobile technology.

We also recognise that whilst it is essential to ensure that appropriate filters and monitoring systems are in place, we should be careful that 'over-blocking' does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Moulton Chapel uses a range of devices including PC's, laptops and IPads. In order to safeguard the pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet filtering – we use software that prevents unauthorised access to illegal website. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in a response to any incident, whichever is sooner.

E-mail filtering - we use software that prevents any infected email to be sent from the school or to be received by the school. Emails are regularly monitored by our ICT support.

Passwords – all staff and pupils will be unable to access any device within the school without the use of a unique username or password / or both.

Anti-Virus – all capable devices will have anti-virus programs on them, and this is monitored and updated by Ark ICT solutions, our technical support service.

Ratified by Governors: December 2024
Next review: Term 2 2027

Moulton Chapel Primary School
01406 380440
enquiries@moultonchapel.lincs.sch.uk

Safe Use

Internet – Use of the internet at school is a privilege, not a right. Internet use will be granted to staff who work within the school and to pupils who have signed and accepted the Acceptable Use Policy.
Internet activity will be monitored to ensure, as much as possible that users are not exposed to illegal or inappropriate websites, including terrorist and extremist material and to ensure, as much as possible, that users do not actively seek access to illegal or inappropriate websites. The outcomes of these checks will be shared with the Headteacher, and logs kept of contraventions.

What will happen in the event of a pupil being exposed to offensive or upsetting material?

If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will respond to the situation quickly by following these steps:

- *All pupils will be taught to switch off the monitor and report what they have seen to the teacher in charge.*
- *Support will be given to the pupil / pupils involved, the Headteacher will inform parents/carers and they will be given an explanation of the course of action the school has taken.*
- *The URL (address) will be reported to the technical support team at ARK*
- *Class teachers will be given a reminder of what to do in this situation.*

E-mails – all staff are reminded that emails are subject to a freedom of information request, and as such the email service is to be used for professional work-based email only. E-mails of a personal nature are not permitted. Similarly, use of personal e-mails for work purposes is not permitted.

How will e-mail be managed?

Pupils will learn how to use e-mail applications and be taught e-mail conventions. Staff and pupils will begin to use e-mail to communicate with others, to request information and to share information.

- *Communications with persons and organisations will be managed to ensure appropriate educational use and the good name of the school is maintained.*
- *The forwarding of chain letters will be banned.*
- *Pupils may send e-mail as part of planned lessons using their e-mail addresses.*
- *E-mail out of school must be approved before sending.*
- *Pupils must not reveal details about themselves or others such as addresses or telephones numbers or arrange to meet anyone in e-mail communications.*
- *Pupils must ask an adult before they open an e-mail so an adult can be present to read received e-mails.*

Photos and videos – digital media such as photos and videos are covered in the schools Use of Photographs policy. All parents are asked to sign a parental consent slip when their child joins the school or when the policy is amended.

School Website – The school has a school website; staff must adhere to these rules before uploading any information to the site:

- *Permission slips (via the school photograph policy) must be consulted before any image or video is uploaded.*
- *There is to be no identification of students using first and last names, first names only to be used.*
- *Where anything may be comment enabled – all comments are to be monitored and moderated.*
- *All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been sought and granted to there is a license which allows for such use.*

***Notice to take down policy** - should it come to the school's attention that there is a resource which has inadvertently been uploaded, and the school does not have permission to use those resources, it will be removed within one working day.*

Ratified by Governors: December 2024
Next review: Term 2 2027

How will publishing on the school website be managed?

The website celebrates good work, promotes the school and publishes resources and information about the school. A school's website can be accessed by anyone on the internet; therefore, the security and safety of the staff and pupils must be maintained.

- *Class teachers will be responsible for organising the information to be entered onto the website.*
- *The point of contact on the school website will be the school's address and telephone number. Home information and individuals email identity should not be published.*
- *Group photos should not have named list of children attached and must only feature those whose parents have given consent for their child's photograph to be published on the website.*

Incidents – Any e-safety incident is brought to the immediate attention of the Headteacher and in her absence the IT Governor. They will then assist any member of staff in taking the appropriate action to deal with the incident and to fill out the incident log (see appendix 1). The incident and follow up actions will be shared with at the next FGB meeting.

Training and curriculum – It is important that the wider school community is sufficiently empowered to stay as risk free as possible whilst using digital technology; this includes awareness of new and emerging issues.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Headteacher. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of IT and all other policy non-compliance must also be reported to the GDPR coordinator who will report incidents to GDPR depending on the severity of the breach.

These could include accidental or unintentional access to unsuitable websites, Internet searches which bring up undesirable content or minor misuse IT. These should be recorded on the incident form in the IT area and the Headteacher made aware of. The incidents will then be assessed in case further action is needed.

All incidents will be brought to the attention of the Curriculum Governors, or the full Governing body through the Headteacher with information on any actions that needed to be taken and how they were resolved.

Cyberbullying

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.

Preventing and Addressing Cyber-Bullying

E-safety practice is advocated at all times in school. At Moulton Chapel Primary School the following will take place:

- *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.*
- *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.*
- *Cyberbullying will be addressed during curriculum IT teaching and PSHE sessions and will be revisited informally through the year.*
- *Safer Internet Day will be used to reinforce messages regarding the safe use of technology.*

- *All staff, governors and volunteers (where appropriate) receive training on cyber bullying, its impact and ways to support pupils, as part of safeguarding training.*
- *Information for parents will be put on newsletters and published in the school's website.*
- *The school signposts support to parents from the website so they are aware how to report it and how they can support children who may be affected.*
- *All children, parents and staff sign an Acceptable Use Agreement*
- *All incidents of cyberbullying must be reported to the Headteacher. This can be done directly to staff or anonymously through class worry boxes.*
- *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.*

Whilst the school recognises that cyberbullying may take place out of school hours, it will wherever possible, step in to mediate a suitable solution.

Peer on Peer Abuse

This school recognises that children sometimes display harmful behaviour themselves and that such incidents or allegations must be referred on for appropriate support and intervention. Such abuse is unacceptable and will not be tolerated. In the context of this policy, this abuse could for example include:

- *'upskirting'*
- *all forms of bullying via electronic devices*
- *aggravated sexting*

To prevent peer-on-peer abuse and address the wider societal factors that can influence behaviour, the school will educate pupils about abuse, its forms and the importance of discussing any concerns and respecting others through the curriculum, assemblies and PSHE lessons.
The school will also ensure that pupils are taught about safeguarding, including online safety, as part of a broad and balanced curriculum in PSHE lessons, RSE and group sessions.
All staff will be aware that pupils of any age and sex are capable of abusing their peers and will never tolerate abuse as "banter" or "part of growing up".
All staff will be aware that peer-on-peer abuse can be manifested in many ways, including sexting or cyberbullying which aims to cause emotional or psychological harm, for example.
Pupils will be made aware of how to raise concerns or make a report and how any reports will be handled – this includes the process for reporting concerns about friends or peers. If a child has been harmed, is in immediate danger or is at risk of harm, a referral will be made to children's social care services (CSCS).

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Details can be found in the Acceptable Use policy.

Pupils Using Mobile Devices in School

Pupils in UKS2 may bring mobile devices into school, with agreement from the Headteacher, but are not permitted to use them during lessons. The phones are only to be brought into school if the child is due to walk independently into the village to go home or to meet their parent or carer. Some children from separated families also bring in their mobile devices if they are staying with the parent.
These should be switched off / silent and be handed in at the school office and collected at the end of the day. 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.

Ratified by Governors: December 2024
Next review: Term 2 2027

Moulton Chapel Primary School
01406 380440
enquiries@moultonchapel.lincs.sch.uk

How the School will Respond to Issues of Misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies on behaviour and acceptable use. 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 IT 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 and staff code of conduct. 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.

Useful websites:
CEOP is a part of the UK police force dedicated to the eradication of child sexual abuse. There is an excellent educational programme, as well as advice and videos for all ages on their website. www.ceop.gov.uk
IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content. www.iwf.org.uk
BBC - a fantastic resource of e-safety information for the younger child. www.bbc.co.uk/cbbc/help/web/staysafe
Cybermentors is all about young people helping and supporting people online. www.cybermentors.org.uk
Digital citizenship is about building safe spaces and communities, understanding how to manage personal information, and about being internet savvy - using your online presence to grow and shape your world in a safe, creative way, and inspiring others to do the same. www.digizen.org

E-Safety (do's and don'ts)

Some simple do's and don'ts for everybody (courtesy of CEOP):

- ✓ *Never give out personal details to online friends that you don't know offline.*
- ✓ *Understand what information is personal: i.e. email address, mobile number, school name, sports club, meeting up arrangements, pictures or videos of yourself, friends or family. Small pieces of information can easily be pieced together to form a comprehensive insight into your personal life and daily activities.*
- ✓ *Think carefully about the information and pictures you post on your profiles. Once published online, anyone can change or share these images.*
- ✓ *It can be easy to forget that the internet is not a private space, and as result sometimes people engage in risky behaviour online.*
- ✓ *Don't post any pictures, videos or information on your profiles, or in chat rooms, that you would not want a parent or carer to see.*
- ✓ *If you receive spam or junk email and texts, never believe the content, reply to them or use them.*
- ✓ *Don't open files that are from people you don't know. You won't know what they contain—it could be a virus, or worse - an inappropriate image or film.*
- ✓ *Understand that some people lie online and that therefore it's better to keep online mates online. Never meet up with any strangers without an adult that you trust.*

Don't forget, it is never too late to tell someone if something or someone makes you feel uncomfortable.

Ratified by Governors: December 2024
Next review: Term 2 2027

Moulton Chapel Primary School
01406 380440
enquiries@moultonchapel.lincs.sch.uk

Moulton Chapel Primary School
E-Safety Incident Log

Date:	Time:	Staff member:
Details of incident		
Where did it occur?		Who did it involve? Staff member child (please circle)
Names of people involved		
Types of incident	Bullying / harassment Online bullying or harassment (cyber bullying) Deliberate bypassing security or access Hacking or virus propagation Racist, sexist, homophobic, religious hate material, pornography Terrorist / extremist materials Other (specify)	
Nature of incident	Deliberate Accidental	
Did the incident involve material being:	Created Viewed Printed Distributed Shown to others Transmitted to others	
Could this incident be considered:	Harassment Grooming Cyberbullying Sexting Breach of AUP Other (specify)	
Action taken:		
Outcome of incident / investigation		
Recommendations		

Signed:

Print name:

Date:

Ratified by Governors: December 2024
Next review: Term 2 2027