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

E-Safety Policy

Introduction

The requirement to ensure that children are able to use the internet and related communication technologies appropriately and safely is addressed as part of the wider duty of care for all who work within our school. We must ensure that we keep children safe and protected from harm both within and outside of school.
Safeguarding is a serious at matter: at Moulton Chapel Primary School we use technology and the Internet across all areas of the curriculum. Online safety, known as E-Safety is an area that is constantly evolving and as such this policy will be reviewed annually or in response to an e-safety incident, whichever is sooner.

The purpose of this policy is twofold:

- *To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.*
- *To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to our pupils or liability to the school.*

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.*

Roles and Responsibilities

Governing Body

The Governing Body are accountable for ensuring the school has effective policies and procedures in place: as such they will:

- *Review this policy at least annually and in response to any e-safety incident to ensure the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents are reported and dealt with appropriately and ensure the policy was effective in managing those incidents.*
- *Appoint one governor (**Mrs Katie Doades**) to have overall responsibility of e-safety at the school who will:*
    - *Keep up to date with emerging risks and threats through technology use.*
    - *Receive regular updates from the HT regarding training, identified risks and incidents.*
    - *Feedback to FGB of any concerns regarding e-safety*

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*
- *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)*
- *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.*

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

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.

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 the information on how they need to keep 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.

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, governing bodies should ensure their school has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of children and

provide them with a safe environment in which to learn, governing bodies should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.
We recognise that whilst filtering and monitoring are an important part of the online safety picture for schools to consider, it is only one part. We need to 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 solution s, our technical support service.

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.*

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

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 must 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.*

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 (katie.arnott@moultonchapel.lincs.sch.uk). 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.

E-safety is embedded into the curriculum; whenever IT is being used in school, staff will ensure that there are positive messages about the safe use of technology and risks as part of pupils learning.

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

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

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.

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

Appendix 1

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 Shown to others Transmitted to others Distributed	
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: