Moulton Chapel Primary School

E-Safety Policy (School Staff)

This policy has been created with a school emphasis using the e-safety policy of Lincolnshire Safeguarding Children's Board (LSCB) and the Acceptable Use of ICT Policy (AUP). This is a minimum requirement to which all school staff should adhere.

Set out below are the recommendations based on those of the LSCB. In a nutshell, Moulton Chapel Primary School's Staff eSafety Policy is:

- **Internet access** - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues.

  It is recognised that under certain circumstances inadvertent access may happen. For example, a school researching the holocaust may produce results with Nazi propaganda. Should you or a student access any of these sites unintentionally you should report the matter to the headteacher so that it can be logged.

  Access to any of the following should be reported to the headteacher or eSafety Officer, and by the headteacher on to Lincolnshire Police: images of child abuse (sometimes incorrectly referred to as child pornography). These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; criminally racist material in the UK.

- **Email** ï staff should use their school email account for all school business.

- **Social Networking** ï All social networking sites are blocked. This will be reviewed from time to time and, should it become educationally beneficial to use a social networking site, a decision about unblocking a particular site would be made. No member of staff should, knowingly, become a ôfriendô with a pupil on a social networking site nor engage in online chat with a pupil.

- **Passwords** - Staff should keep passwords private. Passwords are confidential and individualised to each person. On no account should a member of staff allow a student to use a staff login.

- **Data Protection** - Where a member of staff has to take home sensitive or confidential information sufficient safeguards should be in place to prevent loss or misuse, i.e. is it really necessary to take it all home, can it be encrypted, does it have to be on a USB memory stick which can be easily misplaced.

- **Images and Videos** - Staff and pupils should not upload onto any internet site images or videos of themselves or other staff or pupils without consent.

- **File sharing -** technology such as peer to peer (P2P) and bit torrents is not permitted on the Lincolnshire Schoolsô Network.

- **Use of Personal ICT** ï if essential, personal ICT equipment may be brought in for use within school. Any such use should be stringently checked for up to date anti-virus and malware checkers.

- **School IT equipment –** at the headteacherôs discretion, school IT equipment may be removed from the school site for planning/presentation etc., purposes. A log book is retained in the school office and any equipment removed from site should be recorded out and when returned.

- **Viruses and other malware** - any virus outbreaks are to be reported to the headteacher or eSafety Officer and by them on to Mouchel Helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

Staff should note that internet and email may be subject to monitoring

E-Safety Policy (students)

The use of ICT within schools has enormous benefits to education, however there are reasons why the school and the local authority must put some restrictions in place, such as: ICT equipment is very expensive to buy and maintain; the school and the local authority have a duty of care to ensure that you are safe and that you are not exposed to illegal or inappropriate content. It is hoped that these restrictions do not interfere with your education, but if you feel otherwise you are encouraged to talk to a member of staff to discuss any issues.

Please note that internet and email use may be subject to monitoring.

Use of the Internet - the internet is provided to help you with learning activities such as research, online activities, online educational games and many other things. The internet is not to be used to access anything which is illegal, or anything that someone else may find offensive. If you are unsure, or if you come across anything you feel is inappropriate, you should turn your computer monitor off and let your teacher know.

Logins and Passwords - every person has a different computer login. You should never allow anyone else to use your details.

Social Networking ï We do not allow access to social networking sites (for example Bebo, Facebook, Flickr). Parents should check the access that children have to social networking sites at home, especially giving consideration to the age restrictions that apply to many sites.

If you do use sites at home remember you must not put photos or information about others on line without their permission. Also, it is not advisable to upload pictures or videos of yourself. Videos and pictures can easily be manipulated and used against you. You should never make negative remarks about the school or anyone within the school. Always keep your personal information private to invited friends only and never post personal information such as your full name, date of birth, address, school, phone number etc. Consider using a nickname and only inviting people you know. Beware of fake profiles and people pretending to be somebody else. If something doesnôt feel right follow your instincts and report it to an appropriate adult. Never create a false profile as a joke and pretend to be somebody else. This can have serious consequences.

Some social networking sites have a chat facility. You should never chat to anyone that you donôt know or donôt recognise. It is recommended that you never meet a stranger after meeting them online. If you do want to meet an online ôfriendô, always inform your parents and take one of them with you.

Security - you should never try to bypass any of the security in place. This security is in place to protect you from illegal sites, and to stop others from hacking into other peopleôs accounts.

Copyright - you should never take information from the internet and use it as your own. A lot of information is copyright, which means that it is owned by somebody

else and it is illegal to use this information without permission from the owner. If you are unsure, ask your teacher.

Etiquette ï You have an email account at school. When you are sending a message always be polite and donôt swear. Consider what you are saying, and how it might be read by somebody else. Without emoticons it is difficult to show emotions in things like emails and blogs, and some things you write may be read incorrectly.

Mobile Phones ï We do not allow pupils to have mobile phones in school.

Remember to always keep yourself safe when using your phone at home in the same way as when you are using the internet at home. Never take inappropriate pictures of yourself and send to your friends or upload onto social networking sites. Never forward inappropriate pictures that you have received from somebody else. In some circumstances this can be an illegal act.

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 Policy (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.

E-Safety Policy (recommended steps)

Here are some thoughts and recommended steps for all schools:

1. **Technology** - the two technology tools available to schools to provide assistance in safeguarding are internet filtering and Securus behaviour management.

Internet filtering - take some time to discuss with your technical team or your managed service provider which categories are blocked and which are allowed. Who makes the decision to block or unblock, the technical team or those delivering the curriculum? Are your staff and students being overly blocked through a ñlocked downòsystem or is the system being properly managed? Are there steps in place to have internet sites blocked or unblocked quickly? What do the students think, do they feel they are being overly blocked? Does your school run regular reports to see if there has been any inappropriate inactivity?

Securus behaviour management - this is a new tool which has recently become available to all schools for free (with a one-off training cost). It can help protect students from cyber bullying, grooming, racist and harmful behaviour. The software takes a screenshot of anything it believes may be inappropriate or illegal, based upon pre-defined rules and threshold levels. It then emails this screenshot to a selected person within the school. If your school has this installed, are both staff and students monitored? If you donôt have it installed you should give it serious consideration.

2. **Policies** - the policies within this booklet are a minimum standard and take into account both e-safety and acceptable use. You are free to design your own policy and change to more suitable wording, as long as the context remains. Staff and students should all sign that they understand and accept the policies, and visibility of these policies should also be given to parents.

3. **Training** - are all staff aware of e-safety, not just teaching staff? Are the students aware? You must be aware of your duty of care as a school, and also your requirements under Ofsted. Are there safety training and awareness sessions available for staff, students and parents? If your school is not confident, consider contacting CfBT and using its accredited training sessions.

4. **Guidance** - technology moves at such a pace, and risk taking behaviours evolve into other risks.

Ongoing training and guidance, particularly as part of CPD is a must. Have you signed up to the monthly e-Safety newsletter which will keep you up to date with other training initiatives?

5. **Responsibility** - this lies with the Headteacher and governing body. Are you aware of your responsibilities and duty of care? Has this responsibility been devolved to the technical team? If so, why? These are not technical issues but potentially very serious pastoral ones.