MissionGrove
PRIMARY SCHOOL
RESPECT YOURSELF RESPECT OTHERS

E Safety Policy

Mission Grove Primary School

This Policy has been written for and adopted by
the Governing Body of Mission Grove Primary School.

VISION STATEMENT

For the children at Mission Grove to become well rounded individuals who have drive, passion and the confidence to do their best. Who leave with the skills to succeed and flourish in life. Staff have high expectations of themselves and others and are reflective practitioners. Mission Grove provides security, opportunities and enjoyment for all.

Approved by Governing Body

Date: January 2018

Mission Grove Primary E Safety Policy

E SAFETY POLICY

Mission Grove is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Why do we have an E-Safety Policy?

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Teaching & Learning, Acceptable Use and Safe-guarding.

The purpose of this policy is to:
-Establish the ground rules we have in school for using the Internet and encourage responsible ICT use by all staff and pupils.
- Describe how these fit into the wider context of other policies.
- Demonstrate the methods used to protect and educate the children when using the internet.
- Explain how we will implement e-safety in both administration and curriculum, including a safe and secure network.

Contents

1. *Teaching and Learning*
    1.1 Why is Internet use important?
    1.2 Why does Internet use benefit education?
    1.3 How can Internet use enhance learning?
    1.4 Home School Agreement

2. Managing Systems
    2.1 *Authorised Internet access.*
    2.2 Email
    2.3 Pupil Images
    2.4 Social Networking
    2.5 Personal Data

3. *Handling Risks*
    3.1 Assessing Risks
    3.2 Handling e-safety complaints
    3.3 Cyber- Bullying
    3.4 Red CEOP Button
    3.5 Other E-safety

4. *Communication of policy*
    4.1 Whole School Rules
    4.2 Pupils
    4.3 Staff
    4.4 Parent

Useful Websites

School e-Safety Policy

Our e-safety Policy has been written by the school, building on the Children and Young Peoples' Directorate and Government guidance. It has been agreed by the E-Safety Coordinator, senior management team and approved by governors.

The e-Safety Policy will be reviewed annually.

1. ***Teaching and Learning***

1.1 Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Mission Grove Primary School has a duty to provide pupils with quality Internet access Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

1.2 How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils world-wide;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the Local Authority and DCSF; access to learning wherever and whenever convenient.

1.3 How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2. ***Managing Systems***

2.1 Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet & network access.
- All staff must read and sign the 'Acceptable Use Policy' before using any school ICT resource.

• Parents will be informed that pupils will be provided with supervised Internet access.
• Parents will be asked to sign and return a consent form for pupil access.

2.2 How will email be managed?

• Teacher email addresses will be used in Mission Grove for communication regarding school matters.
•Teachers need to show professionalism and remember they represent the school when sending emails.
• Access in school to external personal email accounts may be blocked.
• Pupils do not have personal school email accounts but class emails, for educational purposes, may be sent from the teachers account by the teacher.
•Pupils need to understand the reasons for using emails, how to use email accounts and send emails safely for those that may have them outside school or will do in the future
• Teachers should not set up any email accounts for pupils.
•The forwarding of chain messages is not permitted.
• Staff emails are monitored and can be accessed by the Head teacher

2.3 Can pupil's images or work be published?

•Still and moving images and sounds add liveliness and interest to a website, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount.
•Although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown.
• Images of a pupil will be published unless parents request otherwise. Pupils also need to be taught the reasons for caution in publishing personal information and images online
• Pupils' full names will not be used anywhere on the website in association with a photograph.
•All parents' sign an agreement to their child's photograph be taken and used for school purposes when joining the school. (Records are kept in the office)Those children that are exempt are clearly known by appropriate teachers and Senior Management.
•For every school trip a further consent is gained for every child to have photographs which may be used on by the school. Class Teacher to be fully aware before trip begins and a record of consent to be kept in case of dispute.

2.4 How will social networking, social media and personal publishing be managed?

• Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content.
• Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.
•Although primary age pupils should not use Facebook, Instagram, Snapchat or similar sites, pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.
• No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present.
• Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.
• Teachers cannot under any circumstances mention any references to their working lives on any social media.
•The school will control access to social media and social networking sites.
• Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
• Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.

• Staff are advised not to run social network spaces for pupil use on a personal basis.
• Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

2.5 How will filtering be managed?

•The School will work with LGFL to ensure that systems to protect pupils are reviewed and improved.
•If staff or pupils discover unsuitable sites, the URL must be reported to the E-Safety co-ordinator or Head Teacher.
•The School's broadband access includes filtering appropriate to the age and maturity of pupils. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
•Any material that staff believe is illegal must be reported to the Head teacher who will inform the appropriate agencies.
•We keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies.
• There are dangers for staff however if personal phones are used to contact pupils or families and therefore this will only be done when authorised by a senior member of staff.
• Abusive messages should be dealt with under the school's behaviour and anti-bullying policy.
• Emerging technologies will be examined for educational benefit and the
Head teacher in consultation with staff will give permission for appropriate use.
• Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text, picture or video messages is forbidden.
• Pupils are not allowed to bring mobile phones into school. Under certain circumstances exceptions can be discussed with the Head teacher, So that pupil mobile phones can be kept in the school office. Parents must complete the permission slip to acknowledge that the school takes no responsibility for phones which are left in the office.

2.6 How should personal data be protected?

•The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly.
•It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.
• The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.
• The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

3. ***Handling Risks***

3.1 How will risks be assessed?

• Mission Grove will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Waltham Forest LA can accept liability for the material accessed, or any consequences resulting from Internet use.
•The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly and after every breech of this policy.

3.2 Handling e-safety Complaints

• Complaints of Internet misuse will be dealt with by the E-safety Coordinator.
• Any complaint about staff misuse must be referred to the Head Teacher.
• Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
• Pupils and parents will be informed of the complaints procedure.

3.3 How will Cyber bullying be managed?

• Cyber bullying is defined as "The use of Information Communication Technology," particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.
•It is essential that pupils, Mission Grove staff and parents and carers understand how Cyber bullying 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. DCSF and Childnet have produced resources and guidance that will be used to give practical advice and guidance on cyber bullying: http://www.digizen.org/cyberbullying
• Cyber bullying (along with all forms of bullying) will not be tolerated in school. All incidents of cyber bullying reported to the school will be recorded.
•There are clear procedures in place to investigate incidents or allegations of bullying:
• Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
•The School will take steps to identify bullying behaviour, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
• Sanctions for those involved in Cyber bullying may include: The perpetrator will be asked to remove any material deemed to be inappropriate or offensive.
•A service provider may be contacted to remove content.
• Internet access may be suspended at school for the user for a period of time.
• Parent/carers will be informed and the Police will be contacted if a criminal offence is suspected.

3.4 Red CEOP Button

All pupils and staff at Mission Grove have been informed about the Red "Report Abuse" Button which is on the school E-safety section of the website. This is a tool that all pupils can use if they ever feel unsafe when using the internet either in school or anywhere in the world.

3.5 Other E-safety Issues

Sexting – Children in Year 5 and 6 will be informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the World Wide Web.

Pornography – many children will come across some type of pornographic content when searching the Internet. Children are taught about what to do if they come across this type of material and who to speak to.

4. Communication of Policy

4.1 Mission Grove E-Safety Code

1. If you are unsure, tell an adult you trust. (Always tell an adult if something makes you uncomfortable, or you are unsure about what to do.)
2. Be nice, even if others aren't. (Treat people online as you would in the playground.)
3. Take care with what you share. (Be careful sharing anything personal, including photos. Ask first.)
4. Remember there could be strangers online too. (Remember stranger danger applies online: people and places are not always what they seem.)

5. Find a balance with how much time you spend online. (Keep a healthy balance between the online and the offline world.)

4.2 Pupils

- E-safety rules are posted in every classroom.
- Children will be informed that Internet use will be monitored.
- Children will sign the e-safety code with the home school agreement.
- Regular lessons will remind pupils of E-safety.
  Including:
    1) Discovery Espresso
    2) Thinkuknow
    3) LGFL Digital Literacy and Citizenship
- E-safety week to highlights importance to pupils in February

4.3 Staff

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that of the e-safety rules and share regularly with pupils.
- Inset training on E-safety

4.4 Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- E-safety booklet discussed at yearly coffee meeting with parents and available all year to give to parents.
- Parent E-safety workshops during e-safety week.

Useful Websites

www.gridclub.com
www.kidsmart.org.uk
www.thinkuknow.co.uk
www.netsmartz.org
www.bizzikid.co.uk

E-safety – learning from home addendum

During school closures and remote learning, ***the same principles of safeguarding, online safety and behaviour apply as in school.*** However, we wish to remind the school community of the existing principles when learning at home.

Mission Grove is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

As per the DfE guidelines, Mission Grove believes:

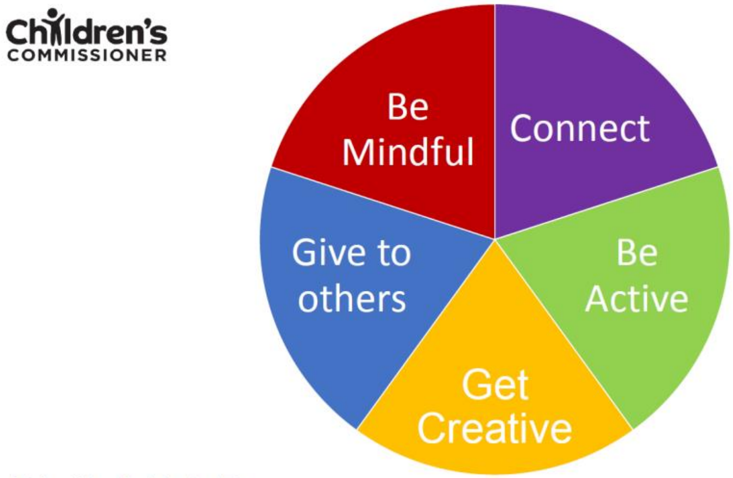
- all pupils should receive a high-quality education that promotes their development and prepares them for the opportunities, responsibilities and experiences of later life.
- the curriculum should be broad and ambitious: all pupils continue to be taught a wide range of subjects, maintaining their choices for further study and employment.
- remote education, where needed, is high quality and aligns as closely as possible with in-school provision

<u>Our safe-guarding principles for remote learning</u>

1. Our staff only use school-registered accounts, never personal accounts
2. Special consideration is made to meet the needs of vulnerable pupils and those with SEND
3. There is always a clear way for pupils and parents to ask questions and get help while learning from home
4. Remote learning is inclusive – arrangements are made for pupils who do not have internet access or an suitable device
5. Our normal safeguarding policy and procedures always apply

<u>Support and advice for parents</u>

We encourage all families learning at home to follow the 'Digital 5 a day'.



Digital 5 A Day

Simple steps to a balanced digital diet and better wellbeing

Finding the right digital balance means enjoying all the fun, exciting and creative things about being online while making sure that we aren't caught doing the same things all the time.

Connect

Message, have fun and play with friends and family both online and offline

Be Active

Take some time off and get active -movement helps boost emotional wellbeing

Get Creative

Don't just browse the internet but use digital tools to create content, to build new skills and discover new passions

Give to Others

Be positive online, report bad content and help others to balance their own 5-a-day

Be Mindful

If time online is causing stress or tiredness then take some time off and ask for help when you need it

Full details here: https://www.childrenscommissioner.gov.uk/our-work/digital/5-a-day/

We encourage families to follow our e-safety code at home, as well as at school (see below).

We encourage parents to set up appropriate controls on all devices at home. Step by step guides on how to do this can be found on the Internet Matters website: https://www.internetmatters.org/parental-controls/

Any parents with an e-safety concern should contact the school for help or advice. Please also refer to LGFL's six top tips for parents (below).

Mission Grove E-safety Code

It's our mission to enjoy the internet safely.

1. If you are unsure, tell an adult you trust.

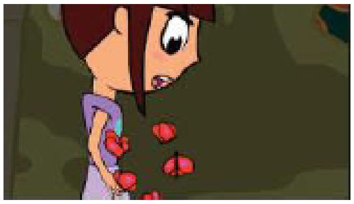
Always tell an adult if something makes you uncomfortable, or you are unsure about what to do.

2. Be nice, even if others aren't.

Treat people online as you would in the playground.

3. Take care with what you share.

Be careful sharing anything personal, including photos. Ask first.



4. Remember there could be strangers online too.

Remember stranger danger applies online: people and places are not always what they seem.

5. Find a balance with how much time you spend online.

Keep a healthy balance between the online and the offline world.

LGfL DigiSafe
Keeping children safe

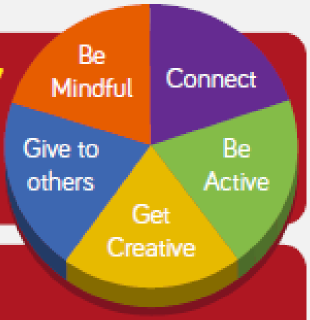
SIX TOP TIPS

To Keep Primary Kids Safe Online During School Closure

Children are bound to spend lots more time on devices during school closure. DON'T FEEL BAD ABOUT IT – lots will be schoolwork or catching up with friends. But there are ways to keep them safe, healthy and happy.

Don't worry about screen time; aim for screen quality

Scrolling through social media isn't the same as making a film or story, or Skyping Grandma. Use the Children's Commissioner's 'Digital Five A Day' to plan or review each day together.



Check the safety settings are turned on

Whether it's your home internet, mobile devices, consoles, apps or games, there are lots of settings to make them safer. The key ones are - can they chat to strangers, can they video chat or 'go live', are their posts public? Internet Matters has hundreds of guides to parental controls.

Get your children to show you their apps and games

You don't need to know all about the latest app or game, but if your child shows you what they are doing and with whom, you'll probably see if it's appropriate or not. Remember 18 games are not more advanced – they are harmful to children! For parent guides to apps, including recommendations for kidsafe apps and video platforms, search for Common Sense Media or NSPCC's NetAware. And why not download the BBC Own It app?

Don't try to hide the news about coronavirus

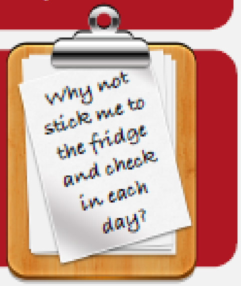
If you don't talk about it, your children might read inappropriate pages, believe scare stories or simply catastrophise in their heads. Why not watch Newsround together and talk about how they feel – there is guidance from Childline to help you.

Remind them of key online safety principles

There are too many to list, but remember human behaviour is the same online and offline. Remind your children to be a good friend, to ask for help if they are worried or if someone is mean, not to get undressed on camera and most important of all… if somebody tells them not to tell or ask for help because it's too late or they will get in trouble, THAT'S A LIE!

If you aren't sure, ASK!

Your school may be able to give you advice, but there are plenty of other places to ask for help as a parent or a child, whether it is advice or help to fix something. Lots of sites are listed at reporting.lgfl.net, including ones to tell your kids about (they might not want to talk to you in the first instance).



Why not stick me to the fridge and check in each day?

You can find anything above by just googling it, or follow us @LGfLDigiSafe on Twitter or Facebook where we regularly share these resources