Menston Primary School

E-SAFEGUARDING POLICY

Menston Primary School
Menston
West Yorkshire
LS29 6LF
Tel: 01943 873180
E-mail: office@menstonprimary.co.uk
Web site: www.menstonprimary.co.uk
Headteacher
Iain Jones

Approved by the Governing Body School Improvement and Standards committee: January 2016
Most recent review by the Senior Leadership Team: November 2019
Date to be reviewed by the Senior Leadership Team: November 2020

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. We want schools to equip their pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world. (Teaching Online Safety in School - June 2019)

Academic year(s)	Designated Safeguarding Lead	Deputy Designated Safeguarding Lead	Computing subject co-ordinator	Nominated Governor	Chair of Governors
2019 - 2021	Iain Jones	Marie Wilson	Amy Dawson	Annet Nottingham	Annet Nottingham

The school will monitor the impact of the policy using:

- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity

Scope of the Policy

This policy applies to all members of the school (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Rationale

Digital technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.
The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

The Risks

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college 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; for example pornography, fake news, racist or radical and extremist views;

• **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying. (Keeping Children Safe in Education September 2019)

The curriculum

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with safe and structured Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of our school's safeguarding provision. Children need the help and support of school staff to recognise and avoid e-safety risks and build their resilience.

The e-safety curriculum at Menston Primary school is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- An e-safety curriculum, which is taught progressively across all year groups. This curriculum is underpinned by the Education for a Connected World framework, which has been developed by the UK Council for Internet Safety and Teaching Online Safety in School (DfE June 2019)
- Key e-safety messages are reinforced in assemblies and through other areas of the curriculum.
- Pupils are taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, sites are checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to search the internet, they use 'safe search' browser and staff are vigilant in monitoring the content of the websites visited.
- Pupils are signposted to relevant online help and advice through visiting sites such as http://www.childnet.com/young-people/primary , https://www.thinkuknow.co.uk and http://www.saferinternet.org.uk/advice-and-resources/young-people/3-11s within lessons.
- Pupils are taught about trusted adults and how they may report things that worry them.
- Digital Leaders, recruited from the pupil body, help to educate other pupils across school in how to keep themselves safe**.**

Parents/ carers

Many parents and carers have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters and web site
- Parents evenings, curriculum evenings, other school events
- High profile events such as Safer Internet Day
- Signposting to relevant web sites such as:
  The UK Safer Internet Centre https://www.saferinternet.org.uk/advice-centre/parents-and-carers
  Childnet International http://www.childnet.com/parents-and-carers
  Common Sense Media https://www.commonsensemedia.org/
  Thinkuknow https://www.thinkuknow.co.uk/parents
- Providing hyperlinks to relevant websites on our school website.

Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- A planned programme of e-safety training will be made available to all staff. This will be regularly updated and reinforced.
- All new staff will receive safeguarding (including e-safety) training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements. All staff sign a Code of Conduct in which they agree to abide by school's e-safeguarding procedures.
- All volunteers and service providers receive safeguarding information as part of their induction and will sign a Code of Conduct in which they agree to abide by school's e-safety procedures.
- This e-safety policy and its updates will be presented to staff as updates are made.
- The e-safeguarding co-ordinator and computing co-ordinator will provide advice, guidance and training to individuals as required.

Roles and Responsibilities

Governors

Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare. Governing bodies and proprietors should ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated. Induction and training should be in line with advice from the local three safeguarding partners. As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place. Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding. (Keeping Children Safe in Education – September 2019)

Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community. The Senior Leadership Team are responsible for responding to any e-safety allegations that are made against a member of staff. Any such incidents will be dealt with in line with the school's disciplinary procedures policies.

The SLT are responsible for ensuring that staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

E-Safeguarding Coordinator

This school has a named member of staff with a day to day responsibility for e-safeguarding, a role which is combined with Child Protection / Safeguarding leadership role.

The e-safeguarding coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing school e-safeguarding policy;
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- provides training and advice for staff;
- liaises with school technical staff in developing and maintaining safe practices and systems;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments (school electronic communications are monitored by https://www.esafeglobal.com/ and receives weekly incident reports);
- deals with e-safety monitoring reports and shares information with Headteacher/ Designated Safeguarding Lead;
- contributes to governing body safeguarding reports

Network Manager

It is the responsibility of the school to ensure that the managed service provider (Primary Technology®) carries out all the e-safety measures outlined below. It is also important that the managed service provider is fully aware of the school e-safeguarding policy and procedures.

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant;
- that the use of the network, internet, remote access & email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and e-safeguarding coordinator for investigation

School Staff

All staff who work in school have responsibility for ensuring that:

- they have an up to date awareness of e-safety matters and of the current e-safeguarding policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement from the Policy on School ICT and Communications Systems
- they report any suspected misuse or problem to the Headteacher or e-safeguarding coordinator for investigation / action/ sanction
- all digital communications with pupils and parents / carers should be on a professional level and only carried out using official school systems

In addition, all teaching and support staff have responsibility for ensuring that:

- pupils understand and follow the Pupil Computer and Internet Agreement
- E-safety issues are embedded in all aspects of the curriculum and taught alongside and within ICT and Computing schemes of work

- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes for dealing with any unsuitable material are followed.

All teaching and teaching support staff are trained in e-safeguarding issues and are aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Vulnerability to radicalisation or extreme viewpoints (see Child Protection Policy)
- Peer on peer abuse
- Sexual violence and sexual harassment between children in schools and colleges (including upskirting)

All staff know the procedures to follow if they are worried that a child or children are at risk of abuse, including online abuse (see Child Protection Policy)

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Computer and Internet Agreement.
- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should know and understand policies on the use of mobile devices and digital cameras.
- Should understand the importance of adopting good e-safety practice when using digital technologies in and out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.
Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events (i.e. not sharing images of other people's children publicly on social media .

TECHNICAL – INFRASTRUCTURE / EQUIPMENT, FILTERING AND MONITORING

- Virus protection will be installed and updated regularly.
- There will be regular reviews and audits of the safety and security of school technical systems by the Network Manager.
- Internet access is filtered for all users. Illegal content is filtered by the school's firewall. Content lists are regularly updated and internet use is logged and regularly monitored.
- Electronic communications are monitored by esafeglobal.com. Weekly reports are sent to the Headteacher and e-safeguarding lead. In addition to this, incident reports are sent as incidents occur.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- All laptops and tablets taken home by staff are encrypted and staff must not leave their devices open and logged in when not in use.

E-mail/ Communications

When using communication technologies the school considers the following as good practice:

- Pupils and staff may only use approved e-mail accounts on the school system whilst in school and communicating on school business.
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses must not be used for these communications. Only the approved systems for text messaging and social media may be used to communicate about school business (Schoolcomms and the school Twitter account).
- Pupils are taught about e-safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and reminded of the need to communicate appropriately when using digital technologies.

Use of Digital and Video Images

- The development of digital imaging technologies has created significant benefits to learning, allowing our staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:
- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection (e.g. for Looked After Children), these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should never be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately clothed and that no-one could reasonably question the intent of the photograph or video.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or social media account.

Social media

The widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, the community, our legal responsibilities and our reputation.

There are legitimate uses of social media within the curriculum and to support student learning. For example, the school has an official Twitter account (@menstonprimary). There are also possibilities for using social media to enhance and develop learning. When using social media for educational purposes, the following practices are observed:

- The school, through Schools Broadband, will control access to social networking sites, and consider how to educate students in their safe use.
- In line with our E-Safety curriculum, pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- In line with our E-Safety curriculum, pupils will be educated not to place personal photos on any social network space without considering how the photo could be used now or in the future.
- In line with our E-Safety curriculum, pupils will be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.
- The ICT and Communications Policy for Staff clearly outlines acceptable use of Social Media. All staff have to sign a receipt for this policy and, in doing so, agree to its terms.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

POLICY DECISIONS

Authorising Internet access

- All staff, volunteers and student placement personnel must read and sign the ICT and Communications Policy for Staff before using any school ICT resource.
- The school will maintain an up to date record of all staff and pupils who are granted access to school ICT systems.
- Parents/carers and children are asked to sign the Computer and Internet Agreement

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school, nor Schools Broadband can accept liability for any material accessed, or any consequences of Internet access.
- Children will be supervised at all times when using the Internet at school - an adult will always be present in the room. Children will not be allowed access to a machine logged on as a staff member.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a member of the Senior Leadership Team.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.
- The school will liaise with local organisations to establish a common approach to e-safeguarding.

This is a working document and will be reviewed regularly. Any amendments will be presented to the Senior Leadership Team (and, where appropriate, the full governing body) for their approval and to staff as part of the regular training programme.

Schedule for Development, Monitoring & Review of this policy

This e-safety policy was approved by the Governing Body:	January 2016
Updates to this policy approved by the Senior Leadership Team	January 2017 February 2018 November 2019
The implementation of this e-safety policy will be monitored by the:	E-safeguarding coordinator, SLT, business manager, safeguarding governor and network manager
The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	annually
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	November 2020
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Bradford Safeguarding Children Partnership safeguarding officer, police, chair of governors
The school will monitor the impact of the policy using:	Logs of reported incidents Surveys / feedback from pupils, parents / carers, staff

Appendix A

E- Safety Rules (to be displayed in all curriculum areas and referred to regularly)

The school has installed computers and internet access to help our learning. These rules will keep to everyone safe:

I will access the school network and internet only with permission from a member of staff.
I will use only my own login, which I will not share with others.
I will not access other people's files.
I will use the computers in school only for school work and homework.
I will not bring memory sticks or other data storage devices into school unless I have permission.
I will only e-mail people I know, or my teacher has approved.
I will ask permission before opening an email and/or attachment sent by someone I don't know.
The messages I send will be polite and sensible.
I will not give my home address or phone number, or arrange to meet someone.
To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like.
I will not use Internet chat except if it is a discussion room that has been set up by my teacher or another member of school staff.
Any work that I display on the school website will be work that I know I would want my family and friends to see.
I understand that the school may check my computer files and may monitor the internet sites I visit.
I understand that if I deliberately break these rules, I could be stopped from using the Internet

Appendix B

MENSTON PRIMARY SCHOOL COMPUTER AND INTERNET AGREEMENT (KEY STAGE 2)

The school has computers and internet access to help our learning.
This agreement will keep everyone safe and help us to be fair to others.

I will take care of the computers and equipment

- I will look after the computer and other ICT equipment. I will return mobile devices to my teacher when I have finished using them.
- I will not copy any software.
- I will not bring files from home to use on the school computer without permission from a member of staff.
- I will not print anything without the permission of a member of staff.

I will be considerate to others

- I will share equipment sensibly.
- I will use only my own login unless asked to share another pupil's by a member of staff.
- I will not access other people's files unless asked to share another pupil's by a member of staff.
- If I accidentally come across unsuitable, dangerous or illegal material I will **immediately** remove it from the screen and tell a teacher, without showing any other pupils.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not try to find out anybody else's password.

I will look after myself sensibly

- I will not give anyone on the internet personal information about myself or others – this includes addresses and phone numbers
- I will access the school network and internet only with permission from a member of staff.
- I will not try to look up things on the internet which I know are not for children. (Your teacher will talk to you about this)
- I will only e-mail people I know and my teacher has approved and I will not open an attachment, or download a file, unless I have permission or know and trust the person who has sent it.
- I will only use the school's computers for schoolwork and homework.
- I will not bring memory sticks or other data storage devices into school unless I have permission.
- I will keep my password secret and only use my own login.
- To help protect other pupils and myself, I will tell a teacher or other trusted adult if I see anything I am unhappy with or I receive messages I do not like.
- I will not use Internet chat except if it is a discussion room that has been set up by my teacher or another member of school staff.
- Any work that I display on the school website will be work that I know I would want my family and friends to see.
- I understand that the school may check my computer files and may monitor the internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers in school.

PUPIL CONTRACT – Key Stage 2

I have read my Computer and Internet Agreement and I know what the school rules are about the use of computers and the internet. I know that if I break these rules there may be serious consequences. For example I may lose the right to use computers in school.

Name:……

Class:……

Signature:……..... Date:…….

PARENT CONTRACT

I have read the Computer and Internet Agreement and understand that there may be consequences if the rules are broken. I have discussed the information with my child and explained its importance.

I understand that while the school will do its best through the filtering system to restrict pupil access to offensive, dangerous or illegal material on the internet or through e-mail, it is also the responsibility of my child to have no involvement in such material.

I give permission for…….. Year……... to be given

access at school to the internet and e-mail and agree to the written terms.

Name:…….

Signature…… Date:……..

Appendix C

MENSTON PRIMARY SCHOOL COMPUTER AND INTERNET AGREEMENT (FOUNDATION/KEY STAGE 1)

The school has computers and internet access to help our learning.
This agreement will keep everyone safe and help us to be fair to others.

I will take care of the computers

- I will look after the computer equipment.
- I will not copy any software.
- I will not bring files from home to use on the school computer.
- I will not print anything without the permission of a member of staff.

I will be considerate to others

- I will share equipment sensibly.
- I always use my own login number and my own file unless a teacher tells me to use a different one.
- I will not try to find out anybody else's password.

I will look after myself sensibly

- I will ask permission of a member of staff before using the computer.
- I will not give anyone on the internet information about myself or others – this includes addresses and phone numbers.
- I will only visit websites that my teacher tells me to.
- I will only e-mail people I know and my teacher has approved.
- To help protect other pupils and myself, I will tell a teacher or other trusted adult if I see anything I am unhappy with or if I receive messages I do not like.
- I will only use the school's computers for schoolwork and homework.
- I will keep my password secret and only use my login.

PUPIL CONTRACT – Foundation and Key Stage 1

An adult has explained my Computer and Internet Agreement to me and I know that there are school rules about the use of computers and the internet. I know that if I break these rules there may be serious consequences. For example I may lose the right to use computers in school.

Name:……

Class:……

Signature:……..... Date:…….

PARENT CONTRACT

I have read the Computer and Internet Agreement and understand that there may be consequences if the rules are broken. I have read and discussed the information with my child and explained its importance.

I understand that while the school will do its best through the filtering system to restrict pupil access to offensive, dangerous or illegal material on the internet or through e-mail, it is also the responsibility of my child to have no involvement in such material.

I give permission for…….. Year……... to be given

access at school to the internet and e-mail and agree to the written terms.

Name:……

Signature…… Date:…….