Olney Middle School

e-Safety Policy

March 2016

Agreed by FGB: 15/03/2015

Updated: 01/08/2017

Updated: 02/09/2019

Review by date: 09/2020

The policy is scheduled for review, as per the above date however if there are legal or statutory changes the policy will need to be reviewed

Author: B Tate

Version: Version 1.3

Olney Middle School E – Safety Policy

This policy also relates to the School Development Plan and to other policies including those for curriculum, ICT, bullying and for safeguarding.

Our e-Safety Policy has been written by the Computing Area of Learning team, Systems Manager and the Safeguarding Officer, building on the national guidance. It has been agreed by the school SLT and the Governing Body.

Date agreed by FGB: 05.03.15

Reviewed date: August 2017

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to support learning and promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- 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 quality Internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use to enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Filtering is provided through a secure GEA network with a Fortigate filter managed by our ICT partners, Silverbug.
- The Fortigate filter is configured to block potential exposure to harmful material in the 'Potentially Laible' category here - https://www.fortiguard.com/static/webfiltering.html - including material that would fall into the definitions of the PREVENT initiative.
- Additional filtering and monitoring is configured for the different groups of devices/platforms in school
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Evaluation of Internet content

- The school will ensure an understanding that copying and subsequent use of Internet derived materials by staff and pupils should comply with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

Managing Information Systems

Information systems security

Local Area Network security issues:

- Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations are secured against user mistakes and deliberate actions.
- Servers are located in the Newton Server cupboard and the Video Suite
- All hardware and operating systems are secure and updated.
- Sophos Virus protection for the whole network is installed and is updated regularly though online access.

Wide Area Network (WAN) security issues:

- All Internet connections are connected via a GEA network using BT fibre broadband (with an ADSL failover for continuity) through a Fortigate filter.
- OMS and Silverbug firewalls and switches are configured to prevent unauthorised access.
- Personal data sent over the Internet or carried on portable media should be encrypted, protected by a password or otherwise secured.
- Portable media may not used by pupils without specific permission followed by a virus check. Staff may use portable media. They are encouraged to virus check these regularly to prevent virus infestation of the school network.
- Unapproved system utilities and executable files will not be allowed in pupil's work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The Systems Manager will ensure that all systems have appropriate capacity, security, redundancy, backups and failsafe at all times.
- The school wifi is GDPR compliant and Guest Wifi access is provided, governed by the IFtL Privacy notice

All staff are provided with e-mail accounts though the school Google Apps for Education installation - e-mail addresses take the form initial.surname@olneymiddle.milton-keynes.sch.uk.(see attached appendix) Pupils e-mail addresses are limited to one per class at the time of writing this policy, this prevents a child being identified. Wider access can be enabled for e-mail use for specific educational projects . Pupils may only use approved e-mail accounts provided through Google Apps

- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain emails is not permitted either by staff or pupils.

- The school email messaging service OMSMail is built on a Wordpress system using the Google Apps email service.

Text messaging

Parents are contacted using Groupcall Messenger who comply with all eSafety and Data Protection guidelines. Mobile numbers are collected from SIMS.net where parents have given permission.

Management of published content

The school has a website. The contact details on the website are the school address, admin e-mail and telephone number. Staff or pupils' personal information is not published, however some staff school email address are published on the website

The head teacher and systems manager will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publication of pupil's images or work.

- Staff will ensure that only digital cameras/phones provided by the school will be used to photograph pupils – if a personal digital camera has been used for specialist purposes, staff will be provided with a school memory card for use in the camera, alternatively images should be removed before the camera leaves the premises
- Staff will ensure that all photographs of pupils are deleted from the school digital cameras as soon as practically possible once transferred.
- Staff will ensure that no photograph or image of pupils will be transferred to personal or home computer systems this also includes personal USB devices.
- Individual pupil's photographs are only published on the school website with parents' written permission – group photos are used in line with the ICO Guidance
- Pupils' full names will not be used anywhere on the school Web site or other unsecured on-line space.
- Pupil file names will not refer to the pupil by name if used for publication.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Management of social networking and personal publishing.

- Pupils will be given opportunities to use the social networking tools available on the School Blog and GoogleApps to enable them to experience social networking in a secure environment. Pupils will not access sites such as Facebook, Instagram etc through the school internet.
- Newsgroups and chat rooms will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their peers and / or their location. Examples would include real name, address, mobile or

landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

- Pupils are 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 eg. house number, street name or school.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others.
- Pupils are advised not to publish specific and detailed private thoughts.
- The School is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- Teachers are expected to behave in a professional manner when using public social media.
- Students use of cloud based computing will be monitored by class teachers during lessons to ensure no inappropriate messages or files are created. Reports of inappropriate use at home will be investigated by the class teacher, ICT Area of learning and systems manager.

Management of filtering

- Internet filtering provided by our ICT partners, SIlverbug through a Fortigate appliance.
- Additional layers of filtering and monitoring are maintained through the Google Apps for Education Administration interface and forced installation of the Securly app for the Chrome/Chromium devices in school.
- Additional filtering and monitoring for the ICT Suite is provided by a pfSense server running a SquidGuard proxy
- Access attempts to unsafe sites and any pupil email content that raises concerns is notified by the apps to the Systems Manager
- If staff or pupils discover unsuitable sites, the URL must be reported to the ICT Coordinator and Systems Manager.
- The Systems Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP (addresses later).
- Any and all such alerts are checked by the Safeguarding lead and dealt with appropriately

How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- The school does not currently enable BYOD
- Staff will always use a school phone where contact with pupils is required.

How should personal data be protected?

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

Data Protection is monitored in school and by the Data Protection Officer for the IFtL Multi Academy Trust of which the school is a member.

The IFtL Privacy Statement is available via the school website.

Policy Decisions

Authorisation of Internet access

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

All staff must read the OMS Acceptable use document before using any school ICT resource.

Risk assessment

- The school 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 Silverbug can accept liability for the material accessed, or any consequences resulting from Internet use.
- 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.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and subsequent legislation.
- Methods to identify, assess and minimise risks will be reviewed regularly.

e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the appropriate authorities handling potentially illegal issues.
    - Sanctions within the school policy include:
        - interview/counselling by senior member of staff
        - informing parents or carers;
        - removal of Internet or computer access for a period.
        - Other responses suggested by the school behaviour policy

Communicating the Policy

Introducing the policy to pupils

- Pupils will be informed that network and Internet use will be monitored.
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- An e-safety module will be included in the Computing and Media programmes covering both school and home use.
- Failure to adhere to the policy may result in the pupil's access to the internet/Learning platform being removed.

Introducing the policy with staff

- All staff in school will be given the School e-Safety Policy and its application and importance explained.
- Staff should be aware that Internet and email traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.
- This will apply equally to supply teachers and student teachers working in school

Parents' support

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website. The pupil will sign the Use of Computers Agreement which is in the school planner
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Appendix 1

Internet use - Possible teaching and learning activities	**Key e-safety issues**
Permission	Pupil and parental consent should be sought prior to Internet access and publication of general images or pupils work online.
Creating web directories to provide easy access to suitable websites.	Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. I am Learning, Google Apps
Publishing pupils' work on school and other websites.	Pupils' full names and other personal information should be omitted. Pupils' work should only be published on moderated sites and by embers of staff.
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.
Communicating ideas	Only chat rooms dedicated to educational use and that

within chat rooms or online forums.	are moderated should be used. Access to other social networking sites is not permitted. Pupils should never give out personal information.
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.

E-safety should be taught regularly in every year group as part of the Computing curriculum. We can put systems in place in schools to minimise the risk to children but we need to educate them to enable them to keep themselves safe in other environments.

e-Safety Contacts and References

BBC Chat Guide

http://www.bbc.co.uk/chatguide/

Becta

http://www.becta.org.uk/schools/esafety (may not be available after March 2011)

Childline

http://www.childline.org.uk/

Child Exploitation & Online Protection Centre

http://www.ceop.gov.uk

e-Safety in Schools

http://www.kenttrustweb.org.uk?esafety

Grid Club and the Cyber Cafe

http://www.gridclub.com

Internet Watch Foundation

http://www.iwf.org.uk/

Internet Safety Zone

http://www.internetsafetyzone.com/

Kidsmart

http://www.kidsmart.org.uk/

NCH – The Children's Charity

http://www.nch.org.uk/information/index.php?i=209

NSPCC

http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Stop Text Bully

www.stoptextbully.com

Think U Know website

http://www.thinkuknow.co.uk/

Virtual Global Taskforce – Report Abuse

http://www.virtualglobaltaskforce.com/

Silverbug support

support@silverbug.com

Appendix 2

Google Supplier Self Certification – Cloud Software Services for Schools

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/404098/Cloud-services-software-dept-advice-Feb_15.pdf (14 pages)

The most up to date version of this policy is available on the school website. If you are reading a hard copy of this policy please check the version on the school website.

OMS February 2015

Updated September 2019

e-safety POLICY

Olney Middle School – 03/15 revised 09/19

Olney Middle School E – Safety Policy

Date agreed by FGB: 15/03/2015

Review date: 01/08/2017 to include additional filtering arrangements

Review date: 02/09/2019 to Include additional filtering arrangements and privacy update

Author: Barbara Tate

The most up to date version of this policy is available on the school website. If you are reading a hard copy of this policy please check the version on the school website