POLICY: E-Safety

Name of School	Mayflower Community Academy
Policy review Date	September 2019
Date of next Review	September 2020
Who reviewed this policy	Computing Lead, Network Manager and Headteacher

Who does the policy apply to?

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

Head teachers are empowered (The Education and Inspections Act 2006), within reason, to regulate the behaviour of pupils when they are off the school site and permits members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. Mayflower Community Academy will deal with such incidents within this policy (and associated behaviour policies) and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Introduction:

What is E-Safety?

E-Safety focuses on the education of children and young people on the benefits and risks of using new technology (including Internet technologies and electronic communications such as mobile phones and wireless technology); providing safeguards and awareness for users to enable them to control their online experiences. Mayflower Community Academy's e-safety policy will operate in conjunction with other policies including those for Safeguarding, Pupil Behaviour, Bullying, Data Protection and Security. We aim to ensure that children and young people are protected from harm and supported to achieve the maximum benefit from new and developing technologies, without risk to themselves or others.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Thorough implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the South West Grid for Learning including the effective management of content filtering.

Mayflower Community Academy has evaluated its level of e-safety in the Ofsted Self Evaluation Form (SEF), as well as reviewing our provision using the ICT Mark Self Review Framework (SRF), containing a number of aspects regarding the school's e-safety policies and practises.

Our e-Safety Policy has been written by the school, building on the South West Grid for Learning guidance. It has been written by the senior management team, taking input from all members of the school community; governing body, LAT advisory board, teachers, support staff, parents and the pupils themselves. The policy has been agreed and approved by all stakeholders in a child's education.

The e-Safety Policy will be reviewed annually. This policy was reviewed September 2019.

Benefits:

The internet and other digital information technologies are compelling devices and have become an essential part to the lives of children and young people in today's society. Electronic communication opens up new opportunities for everyone; helping teachers and pupils share and learn from each other. These technologies can stimulate discussion and creativity, whilst increasing awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The 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.

The effective and safe use of these innovative and progressive technologies, has proven to raise self-esteem and impact directly on pupil progress.

Why is Internet Use Important?

Internet use is an integral part of everyday life at Mayflower Community Academy; for both pupils and teachers. It raises educational standards, promotes pupil achievement, supports the professional work of staff and enhances the school's management and administration systems.

As part of the statutory curriculum, it is a necessity for effective learning. Access to the Internet is therefore an entitlement for pupils, who need guidance and development in a responsible and mature approach to its use. Our school has a duty of care in providing pupils with quality and safe Internet access.

The internet is a powerful tool and we actively encourage it's usage outside of school. However, children will need to learn how to evaluate and judge Internet information; taking care of their own safety and security.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Headteacher, who will be able to add the site to the school filter list.

- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved e-mail accounts on the school system.
- 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.
- If whole class or group e-mail addresses are used in school, this will be monitored by the class teacher.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations is written carefully and authorised by the class teacher before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking

- We will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils are advised not to place personal photos on any social network space.
- Pupils are advised on security and encouraged to set effective passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- For greater detail, please refer to the schools Social Media policy

Video Conferencing

- Videoconferencing will be appropriately supervised for the pupils' age.

Managing Emerging Technologies

- 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 for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils/ parents is required.

Published Content and the School Web Site

- The contact details on the Web site will be the school address, e-mail and telephone number.
- Staff or pupils personal information will not be published.

- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully, in accordance with Child Protection regulations.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.
- For further information on taking and publishing images of children, please refer to our 'School Policy for safe use of photographs.

Communications

Mayflower Community Academy is thorough in assessing the benefits and risks of the ever-increasing development of communications technologies. Therefore, the following table, for usage of such devices, considers how they can both enhance and pose risk to a child's educational experience.

	Staff & other				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓				✓			
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time in designated areas	✓							✓
Taking photos on mobile phones				✓				✓
Taking educational photos on school tablets	✓						✓	
Removal of school tablets school site				✓				✓
Use of hand held devices e.g. PDAs, PSPs				✓				✓
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails				✓			✓	
Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs	✓						✓	

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the LAT advisory board can accept liability for the material accessed, or any consequences of Internet access.
- 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.

Technical – infrastructure / equipment, filtering and monitoring

Mayflower Community Academy will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible. We will ensure that the policies and procedures approved within this policy are implemented.

School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and any relevant Learning Academies Trust E-Safety Policy and guidance.

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager.
- All users will be provided with a username and password by the Network manager who will keep an up to date record of users and their usernames. This is in accordance with the GDPR guidance.
- The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and kept in a secure place (e.g. school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGfL.
- In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Any filtering issues should be reported immediately and an E-Safety incident report form should be completed in the event of inappropriate content being accessed.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems.
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager/ Headteacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files by users.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place allows staff to / forbids staff from installing programmes on school workstations / portable devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.

Curriculum

- E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager and Headteacher can, if agreed, temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Communication of Policy

Pupils

- Pupils will be informed that Internet use will be monitored.
- A planned e-safety programme should be provided as part of Computing / PSHE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for the safe use of ICT systems / internet will be posted in all rooms and on individual laptop trolleys.

- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Staff

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- An audit of the e-safety training needs will be included as part of the general ICT training needs review process. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable User Policies.
- The Head teacher/Network manager will receive regular updates through attendance at SWGfL / LAT advisory board / other information / training sessions and by reviewing guidance documents released by BECTA / SWGfL / and others.
- The Head teacher/Network manager/Computing Lead will provide advice / guidance / training as required to individuals as required.
- Discretion and professional conduct is essential at all times.

Staff Equipment / Device Policy

- Staff are permitted to use their own computing equipment (<u>not</u> including mobile phones) to work with however **NO** data pertaining to pupils or personal information of other persons / staff may be stored locally upon that system. A VPN and storage drives are provided for such storage both on and off the site. Similarly data stored upon external storage or removable drives is not permitted unless encrypted / password protected.
- Equipment used must first be presented to the school technician in order to assess suitability and to ensure the necessary security levels are being observed (both password protection and AV software). Sophos enterprise can be provided where no anti-virus / malware protection is present.
- Staff must be aware that personal computing items if used for school purposes are done so at their own risk in terms of damage or loss.

Potential and Actual Breaches of the Code of Conduct

In instances where there has been a breach of the terms of this policy by an employee of the school, the following will apply:

Any breaches of this policy by an employee of the school will be ***fully investigated***. Where it is found that there has been a breach of the policy this may result in ***action being taken under the Disciplinary Procedure***. Depending on the circumstances a breach of this policy may be ***viewed as misconduct*** which could result in ***disciplinary action*** being taken or gross misconduct which may result in summary ***dismissal.***

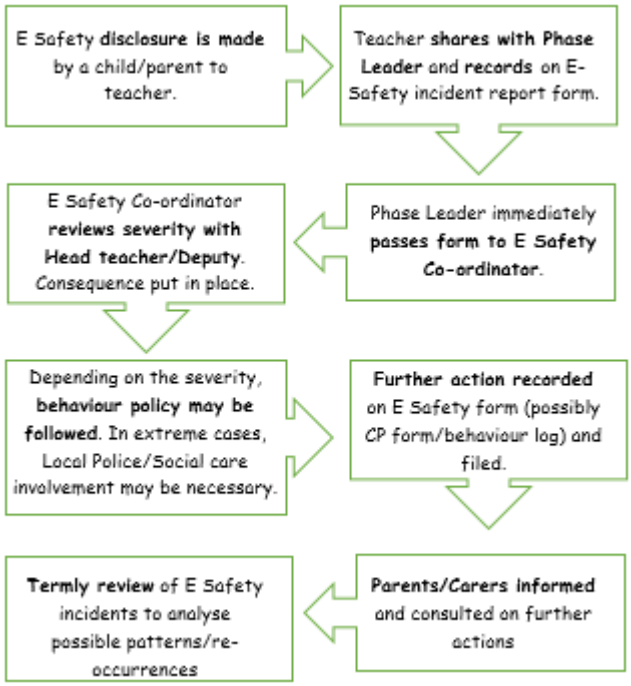
Any breach of this policy by a stakeholder who is not an employee of the school the Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school Web site (where they can be referred to the SWGfL Safe website).
- Parents evenings

All pupils/staff and parents will be required to sign an acceptable use policy agreement

Responding to incidents of misuse/concerns:



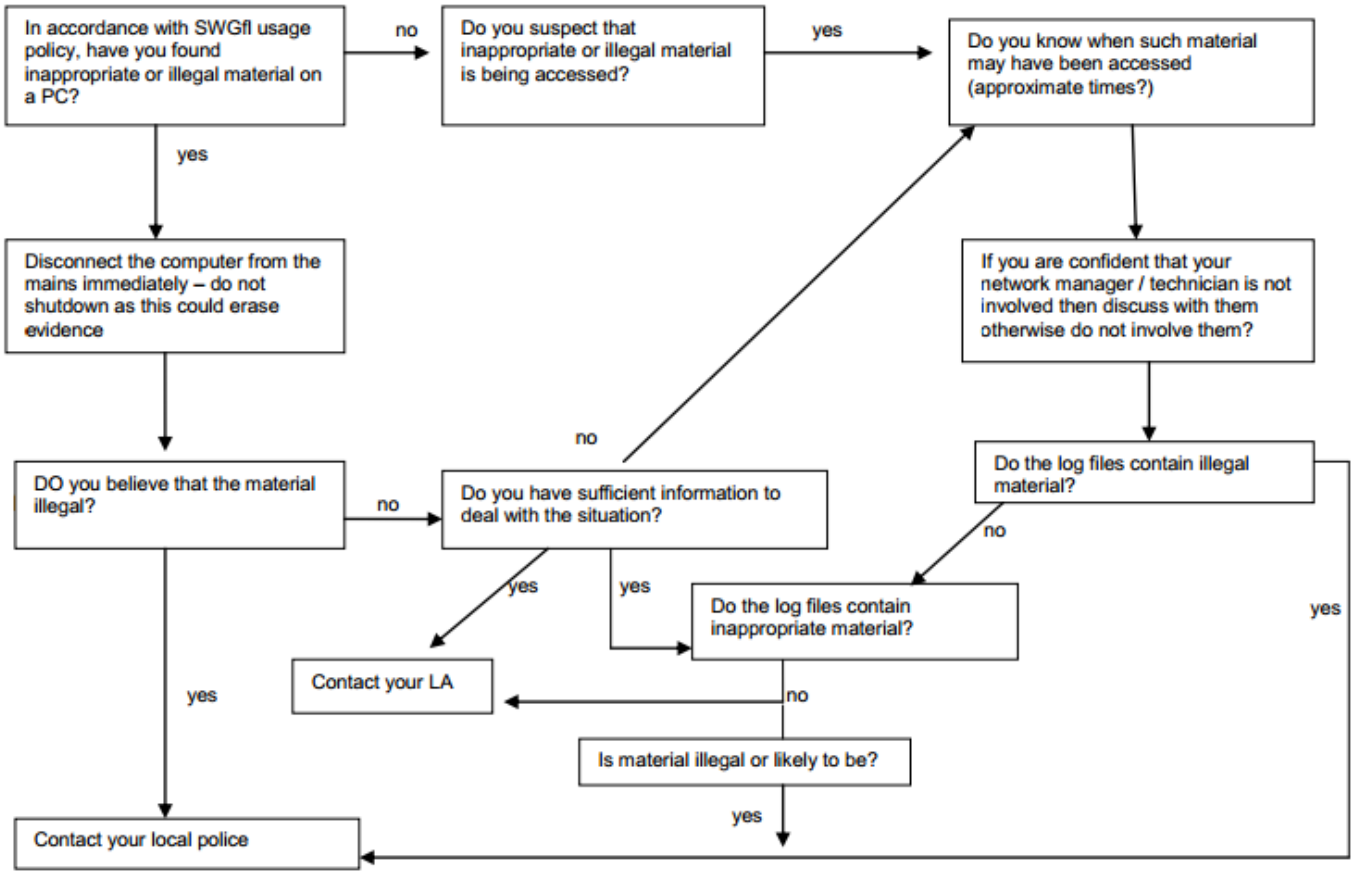
If any apparent or actual misuse appears to involve illegal activity i.e.

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

The SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow.

Flowchart for responding to e-safety incidents in school

Flowchart for responding to e-safety incidents in school



Resources:

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips –for parents and school staff. A comprehensive list of these resources (and those available from other organisations) is available on the "SWGfL Safe" website:

http://www.swgfl.org.uk/safety/safetyresources.asp?page=schoolst_resources&audienceid=3

Links to other resource providers:

Kidsmart: http://www.kidsmart.org.uk/default.aspx

Know It All - http://www.childnet-int.org/kia/

Cybersmart - http://www.cybersmartcurriculum.org/home/

NCH - https://www.stopbullying.gov/cyberbullying/what-is-it/index.html

Internet Watch Foundation: http://www.iwf.org.uk/media/literature.htm

Digizen – cyber-bullying films: http://www.digizen.org/cyberbullying/film.aspx

London Grid for Learning: https://www.lgfl.net/online-safety/

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.