ROBERT MELLORS PRIMARY ACADEMY

E-Safety Policy

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 2018

Introduction

At Mellors Primary Academy we are committed to ensuring that children learn how to use computers, ICT and modern technologies safely so that they:

- Are able to use ICT safely to support their learning in school
- Know how to use a range of ICT equipment safely
- Are able to use ICT and modern technologies outside school in a safe manner, including using ICT as a tool for communication
- Are prepared for the constant changes in the world of technology and understand how to use new and emerging technologies in a safe manner
- Know what to do if they feel unsafe when it comes to using technology and ICT

This policy outlines the steps the school takes to protect children from harm when using ICT and also how the school proactively encourages children to develop a safe approach to using ICT whether in school or at home.

The Law

Our E-Safety Policy has been written by the school, using advice from HCC and government guidance. The Policy is part of the school's Strategic Development Plan and related to other policies including Positive Learning, Safeguarding and Data Protection policies.

As legislation is often amended and new regulations introduced the references made in this policy may be superseded. For an up to date list of legislation applying to schools please refer to the Department for Education website at www.education.gov.uk/schools.

Policy Development

The E-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, Anti-bullying and safeguarding children.

- Our policy has been written with full consultation from staff in school, parents/carers, governors and young people.
- It has been agreed by senior managers and approved by governors
- The policy and its implementation will be reviewed annually.
- It is available to read or download on our school website or you could request a hard copy from the school office.

Roles and Responsibilities

The Headteacher, alongside the E-safety coordinator (Andrew Emsley) will:

- Ensure the policy is implemented, communicated and compliance with the policy is monitored
- Ensure staff training in e-safety is provided and updated annually as part of safeguarding training
- Ensure immediate action is always taken if any risks or dangers are identified i.e. reporting of inappropriate websites
- Ensure that all reported incidents of cyber bullying are investigated
- Ensure appropriate web filtering software is used to protect users from potentially damaging/offensive material

Teachers and Staff will:

- Keep passwords private and only use their own login details, which are stored securely
- Monitor and supervise pupils' internet usage and use of other ITresources
- Adhere to the Acceptable Use Agreement
- Promote e-safety and teach e-safety units as part of computing curriculum
- Engage in e-safety training
- Only download attachments/material onto the school system if they are from a trusted source
- When capturing images, videos or sound clips of children, only use school cameras or recording devices

It is essential that pupils, parents/carers and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of staff members and the reputation of the school and the County Council are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Governors will:

- Ensure that the school is implementing this policy effectively
- Adhere to the acceptable use agreement when in school
- Have due regard for the importance of e-safety in school

Teaching and Learning

Why internet and digital communications are important.

- The purpose of any technology in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- Our school has a duty to provide students with a quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet, including the skills of knowledge location, retrieval and evaluation.
- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- pupils will be shown how to publish and present information appropriately to a wider audience.
- They will be taught what internet use is acceptable and what is not and given clear objectives for use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- They will be taught how to report unpleasant internet content including cyberbullying or unwanted contact. This will include using the CEOP icon.
- Issues such as Cyberbullying and e-safety will be built into the curriculum to encourage self-efficacy and resilience. Some children who have had problems or with additional needs may need additional support.

The school will actively teach E-safety at an age-appropriate level. The school follows government guidance (including Education for a Connected World framework) allowing coverage of: what should and shouldn't be shared online, password control and cyber bullying among other topics. E-safety will also be embedded throughout learning whenever children are using ICT in other lessons.

Monitoring safe and secure systems

Internet access is regulated by RM UNIFY filtered broadband connection which blocks access to unsuitable websites in accordance with the UK Safer Internet Centre guidance. Antivirus software has been installed on all computers and is to be maintained and updated regularly. Staff passwords are changed regularly and must be strong passwords. Staff take responsibility for safeguarding confidential data saved to laptops, ie use ofs trong passwords. If personal data has to be saved to other media, eg data sticks or CDs, it is to be encrypted or strong password protected, staff have been trained to use OneDrive to ensure data remain secure and password protected at all times. Staff with access to the ICT systems containing confidential and personal data are to ensure that such data is properly protected at all times.

Safe use of the Internet and Web Filtering

- All staff and pupils will have access to the internet through the school's network
- All staff, volunteers who have use of the school's IT equipment, must read and sign the Staff Acceptable Use Agreement.
- All children must read and sign the Pupil Acceptable Use Agreement.
- If a site containing inappropriate material is encountered, children must report it to an adult who will report it to the Headteacher or E-Safety Coordinator to pass to CITY ICT
- If an adult finds a site that they consider unsuitable they should report it to the Headteacher or E-Safety Coordinator

The use of Email

All teaching and support staff are provided with a school email address. Staff should use this address when sending work-related emails All emails should be professional in nature and staff should be aware that all emails can be retrieved at a later date should this be necessary. Staff emails should never be used to forward 'chain' or 'junk' email. Staff should not communicate with pupils via email.

The school website

- The school web site complies with statutory DFE requirements
- Images that include pupils will be selected carefully and only used if parents have given permission for such images to be posted on line.

Social Networking, Social Media and Personal Publishing (blogging)

The school recognises that it has a duty to help keep children safe when they are accessing such sites at home, and to this end the school will cover such issues within the curriculum. Pupils will not access social networking sites, e.g. Facebook or Twitter in school. They will be taught about how to stay safe when using such sites at home.

Staff private use of social media:

- No reference should be made in social media to students / pupils, parents /carers / school staff or issues / situations related to the school
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- Staff are not permitted to maintain a Social Media relationship with any pupil, current or alumni until such time that the pupil turns 18.

The Use of Cameras, Video and Audio Recording Equipment

Staff may only use the school's photographic or video devices to support school trips and curriculum activities. Photos should only be uploaded to the school system. They should never upload images to the internet unless specific arrangements have been agreed with the Headteacher or Deputy Headteacher, nor circulate them in electronic form outside the school. It is never acceptable to use photographic or video devices in changing rooms or toilets

Personal mobile phones and mobile devices

- Use of mobiles is discouraged throughout the school, particularly in certain areas. The areas which should be considered most vulnerable include: toilets and changing areas, including where children change for swimming.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring at the direction of the head teacher.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Management of online safety incidents

There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions; all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;

- Support is actively sought from other agencies as needed (i.e. MASH, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform MASH.

Working in Partnership with Parents

Parents' attention will be drawn to the e-safety policy through the school newsletters, information evenings and on the school website. A partnership approach with parents will be encouraged. Parents will be requested to sign an Acceptable Use Agreement as part of the Home School Agreement on entry to the school.

Protecting School Staff

In order to protect school staff we require that parents do not comment on school issues or staff using social networking sites. Any concerns or complaints should be discussed directly with the school. The school will take action if there is evidence that inappropriate comments about staff have been placed on the internet in a public arena.

Safeguarding – scope of this policy

(See also Safeguarding and behaviour policies)
The Education and Inspections Act 2006 empowers the Head Teacher 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 cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's Behaviour Management Policy.

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 e-safety behaviour that take place out of school.