Milton Keynes Education Trust

Heronsgate

Online Safety Policy

Revision	Date	Author	Comments
Legal Issues (Pg 8)	06/01/2020	EW	Updated to include Keeping Children Safe in Education 2019 guidance.

Contents

POLICY

Introduction: Milton Keynes Safeguarding Children Board - ONLINE SAFETY in MILTON KEYNES 2011

The aim of the Milton Keynes Safeguarding Children Board ONLINE SAFETY policy is to inform and enable a broad understanding of the key issues and take every opportunity, in the school and in the home, to ensure that young people do not come into contact with the wrong people or inappropriate behaviour.

This approach in the *real* world is just as significant in the *virtual* world. A virtual world is, in the main, a digital experience populated by real people. Whenever we are responsible for young people, or those in society who are vulnerable, then we have a duty to care for them, who they meet and what they experience.

Online Safety is an issue that affects and involves every child, every young person, every parent/carer and every professional. It is a very broad area that demands constant attention and review.

The Milton Keynes Safeguarding Children Board is a multi agency partnership that has statutory responsibility to co-ordinate local safeguarding activity and to ensure its effectiveness. It is anticipated that schools will already have a number of processes in place that are designed to provide a safe and secure environment for use of electronic communications.

As technology and its application continue to develop the Board will regularly review and update this guidance

The context:

The functions of an LSCB are set out in primary legislation *(Children Act 2004)* and regulations *(Local Safeguarding Children Regulations 2006)* and in *Working Together to Safeguard Children (DCSF 2010 ch3).* The core objectives of the LSCB are:

a. To co-ordinate what is done by each person or body represented on the Board for the purposes of safeguarding and promoting the welfare of children in the area of the authority; and

b. To ensure the effectiveness of what is done by each such person or body for that purpose

Safeguarding and promoting the welfare of children includes protecting children from harm. This includes risks posed by inappropriate use of the internet and other electronic media. The digital world in which children and young people now live provides unprecedented opportunities for educational and social learning and development. However these technologies can pose a variety of risks to their safety and wellbeing. Risks might include:

a. Access to illegal, harmful or inappropriate images or other content

b. Unauthorised access to/loss of/sharing of personal information

c. The risk of being subject to grooming by those with whom they make contact on the internet. Research shows that those in possession of indecent images of children are likely to be involved in actual child abuse

d. The sharing/distribution of personal images without an individual's consent or knowledge

e. Inappropriate communication/contact with others, including strangers, e.g. in use of chat rooms, instant messaging, text messaging and mobile phones.

f. Cyber-bullying

g. Access to unsuitable video/internet games

h. An inability to evaluate the quality, accuracy and relevance of information on the internet

i. Plagiarism and copyright infringement

j. Illegal downloading of music or video files

k. The potential for excessive use which may impact on the social and emotional development and learning of the young person

l. Commercial exploitation

m. Risks cannot be completely eliminated and therefore work focuses on awareness-raising, prevention and equipping children and young people to deal with the risks.

The approach

1. Providing children and young people (CYP) with information and resources to use the internet and other media safely and protect themselves.

2. Equipping parents and carers with knowledge and tools to protect CYP.

3. Equipping professionals and others who work with CYP with the information and tools to help CYP and parents/carers to use electronic media safely.

Schools and Other Settings:

National guidance produced by Becta (British Educational Communications and Technology Agency) *Safeguarding Children in a Digital World (2008)* defined expectations that schools should take a lead role in informing children and their parents/carers about the issues and risks associated with the use of digital technologies.

Whilst Becta no longer exists, this expectation has become embedded and is included in inspection evaluations. The lead responsibility of schools was reinforced in the recommendations of the Byron Review *Safer Children in a Digital World (2008)*.

Responsibilities

Governing body

- Developing and maintaining an awareness of the benefits, risks and issues of use of electronic communications.
- Regularly reviewing Online Safety incidents.
- Ensuring Online Safety policies, procedures, responsibilities, technological tools and education programme are regularly reviewed as part of child protection and health and safety.
- Developing and maintaining an understanding of Online Safety policies, systems and procedures.
- Contributing to the development of Online Safety policies.
- Ensuring access to relevant training for all school staff.
- Making appropriate funding available for training and resourcing Online Safety.
- Supporting the Online Safety co-ordinator in the development of an e-safe culture.
- Promoting Online Safety to parents and carers.

Headteacher and senior management team

- Developing, owning and promoting the Online Safety vision to all stakeholders.
- Supporting the Online Safety co-ordinator in the development of an e-safe culture.
- Making appropriate resources available to support the development of an e-safe culture.
- Receiving and regularly reviewing Online Safety incident logs.
- Regularly reviewing Online Safety policies, procedures, technological tools and education programmes as part of child protection and health and safety
- Supporting the Online Safety co-ordinator in the appropriate escalation of Online Safety incidents.
- Taking ultimate responsibility for Online Safety incidents.

Online Safety Co-ordinator

- Developing an e-safe culture under the direction of the management team and acting as a named point of contact on all Online Safety issues.
- Ensuring that Online Safety is embedded within continuing professional development (CPD) for staff and co-ordinating training as appropriate.
- Ensuring that Online Safety is embedded across the curriculum (or other learning activities) as appropriate.
- Ensuring that Online Safety is promoted to parents and carers, and other users of network resources. Maintaining an Online Safety incident log.
- Monitoring and reporting on Online Safety issues to the management team, and other agencies as appropriate.
- Developing an understanding of the relevant legislation.
- Reviewing and updating Online Safety policies and procedures on a regular basis.

Children and young people

- Contributing to the development of Online Safety policies.
- Taking responsibility for keeping themselves – and others – safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.
- Respecting the feelings, rights, values and intellectual property of others.
- Seeking help from a trusted adult if things go wrong, and supporting others who may be experiencing Online Safety issues.
- Discussing Online Safety issues with parents and carers in an open and honest way.

Teaching and support staff

- Contributing to the development of Online Safety policies.
- Taking responsibility for the security of systems and data.
- Having an awareness of Online Safety issues, and how they relate to the children in their care. Modelling good practice in using new and emerging technologies, emphasising positive learning opportunities rather than focusing on negatives.
- Embedding Online Safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action.
- Knowing when and how to escalate Online Safety issues.
- Maintaining a professional level of conduct in their personal use of technology, both within and outside school.
- Taking personal responsibility for their professional development in this area, including personal use of social media

- Maintaining a professional level of conduct in their personal use of technology and social media, both within and outside school and asking for support if needed
- Taking personal responsibility for their professional development in this area.

Parents and carers

- Contributing to the development of Online Safety policies.
- Using learning platforms, and other network resources, safely and appropriately.
- Discussing Online Safety issues with their children, supporting the school in its Online Safety approaches and reinforcing appropriate behaviours at home.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Modelling appropriate uses of new and emerging technology.
- Liaising with school if they suspect, or have identified, that their child is conducting risky behaviour online.

Legal Issues

A comprehensive list of relevant legislation can be found in the Becta document *Online Safety: Developing whole-school policies to support effective practice (2006)*, but key legislation includes:

- The Education Act 2006 gave Governors a duty of well-being for pupils. This includes physical and mental health and emotional well-being and protection from harm and neglect.
- The Computer Misuse Act 1990 makes it a criminal offence to cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer.
- The Sexual Offences Act 2003 makes it an offence to 'groom' children, including through the use of digital communications.
- The Protection of Children Act 1978 and the Criminal Justice Act 1988 make it an offence to take, distribute and possess indecent images of children.
- The Malicious Communications Act 1988 and Protection from Harassment Act 1997 include, harassment, bullying and cyberstalking. Cyber bullying is simply one method amongst the many used for bullying.
- The Department for Education has published a revised 'Keeping Children Safe in Education (2019)' (KCSIE) document and has updated its guidance on peer-on-peer abuse for the new academic year.

Schools need to protect pupils and staff but also to protect themselves from legal challenge. Schools can help protect themselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised". However, schools should be aware that a disclaimer is not sufficient to protect from a claim of personal injury for which the school leadership could be liable; the school needs to ensure that all reasonable actions have been taken to protect users. Individuals' rights to freedom of speech and freedom of choice must be observed, but these need to be balanced against the need to protect younger users.

It is vitally important that parents understand the safeguards that are in place before pupils use digital communications at school. This is important for two reasons.

- Firstly parents understand that their children are using a medium which may cause them to come into contact with material that may be offensive etc.
- Secondly, pupil's usage of the Internet and email will be monitored. Unauthorised monitoring of such usage may bring the school and LA into conflict with the Human Rights Act so far as privacy is concerned.

While there is no statutory requirement for parents to sign acceptable use policies, schools may wish to consider this option. A signed acceptable use form, administered as part of the enrolment process or as part of the home–school agreement, acknowledges the fact that a parent has received the information, and that they and their children are aware of the rules. In addition, it may be appropriate for older students to agree to the rules themselves. However, the language of the rules must be appropriate to the age and understanding of the children.

Parents need to sign to show their acceptance that:

- their child will be using digital technologies with all reasonable safeguards in place
- they understand that no technical safeguard can be 100% effective in preventing Online Safety incidents

Explicit consent should be obtained before any images of pupils are published by the school in any way. There should be a positive expression of informed consent.

Heronsgate Rational:

> *"Children and young people need to be empowered to keep themselves safe – this isn't just about a top-down approach. Children will be children – pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim."*
>
> *Dr Tanya Byron*
> *Byron Review: Safer children in a digital world*

Online Safety encompasses the use of the internet and a range of other new technologies. There are many methods and devices for accessing the internet and online services, and their availability to children and young people is increasing. Modes of access include desktop and laptop computers, mobile phones, other handheld devices such as personal digital assistants (PDAs) and interactive games consoles, both fixed and handheld. As a consequence learning will be less dependent upon location and will be able to take place 'anytime, anywhere' at the point of need.

We use Online Safety, and related terms such as 'online', 'communication technologies' and 'digital technologies' to refer to all fixed and mobile technologies that children may encounter, now and in the future, which might pose Online Safety risks. We try to avoid using the term 'ICT' when talking about Online Safety as this implies that it is a technical issue – which is not the case. The primary focus of Online Safety is child protection; the issues should never be passed solely to technical staff to address. Online Safety is essentially about creating a safe working environment when using new technologies. It is regularly associated with the use of the internet, but not exclusively, and it does involve adults as well as children.

It is impossible to control access across all these devices in all situations where they might be used by children and young people. However, if children and young people can learn to become safe and discriminating users of technology, wherever and whenever they use it, they will be better placed to protect themselves against the risks and challenges they may encounter.

Online Safety and Prevent

The Prevent strategy states that all children and young people need to be safe from terrorist and online extremist materials when accessing school internet. Please see the school's Safeguarding policy and report to the Safeguarding Officers if concerns are raised regarding Online Safety and Prevent.

Online Safety Risks

The Byron review classified Online Safety risks as involving **content, contact** and **conduct**. A child may be a recipient, participant or actor in online activities posing risk, as illustrated in the table below.

	Commercial	**Aggressive**	**Sexual**	**Values**
Content [child as recipient]	Adverts Spam Sponsorship Personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading information or advice
Contact [child as participant]	Tracking (monitoring, by remotely placing software on a child's PC, activity such as web site visits Harvesting (collecting from a number of web sites) personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct [child as actor]	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading information/advice

[Table developed by the EUKids Online project and referenced in paragraph 1.3 of the Byron Review]

The table illustrates that Online Safety risks are posed more by behaviours and values online than the technology itself. Rather than restricting access to technology, we need to empower learners to develop safe and responsible online behaviours to protect themselves whenever and wherever they go online.

Children will experiment online and while their confidence and enthusiasm for using new technologies may be high, their understanding of the opportunities and risks may be low, alongside their ability to respond to any risks they encounter. Schools now need to focus on a model of empowerment, equipping children with the skills and knowledge they need to use technology safely and responsibly and to manage the risks.

PRACTICE:

A safe ICT learning environment schools should include:

- An infrastructure of whole-school awareness, designated responsibilities, policies and procedures.
- An effective range of technological tools.
- A comprehensive internet safety education programme for the whole school community.
- A review process which continually monitors the effectiveness of all the infrastructure, the tools and the education programme.

(a) Whole –school infrastructure

- Children and staff are aware of the issues, how the issues impact upon the school environment and what is safe and responsible behaviour when online. There will be an adult present when children are using ICT equipment to monitor and supervise its use.

- There is designate the senior management team member responsible for safeguarding with responsibility for Online Safety – the Online Safety Co-ordinator (Assistant Headteacher).

(b) Effective range of technological tools

There are a number of technological tools that are used to safeguard users and the systems, such as:

- Firewall.
- Virus protection.
- Monitoring systems – for example, on what has been downloaded, by whom and where it has been stored.
- Filtering and content control – to minimise access to inappropriate content.
- Secure remote access – enabling only authorised users to access the school network from remote locations such as home.

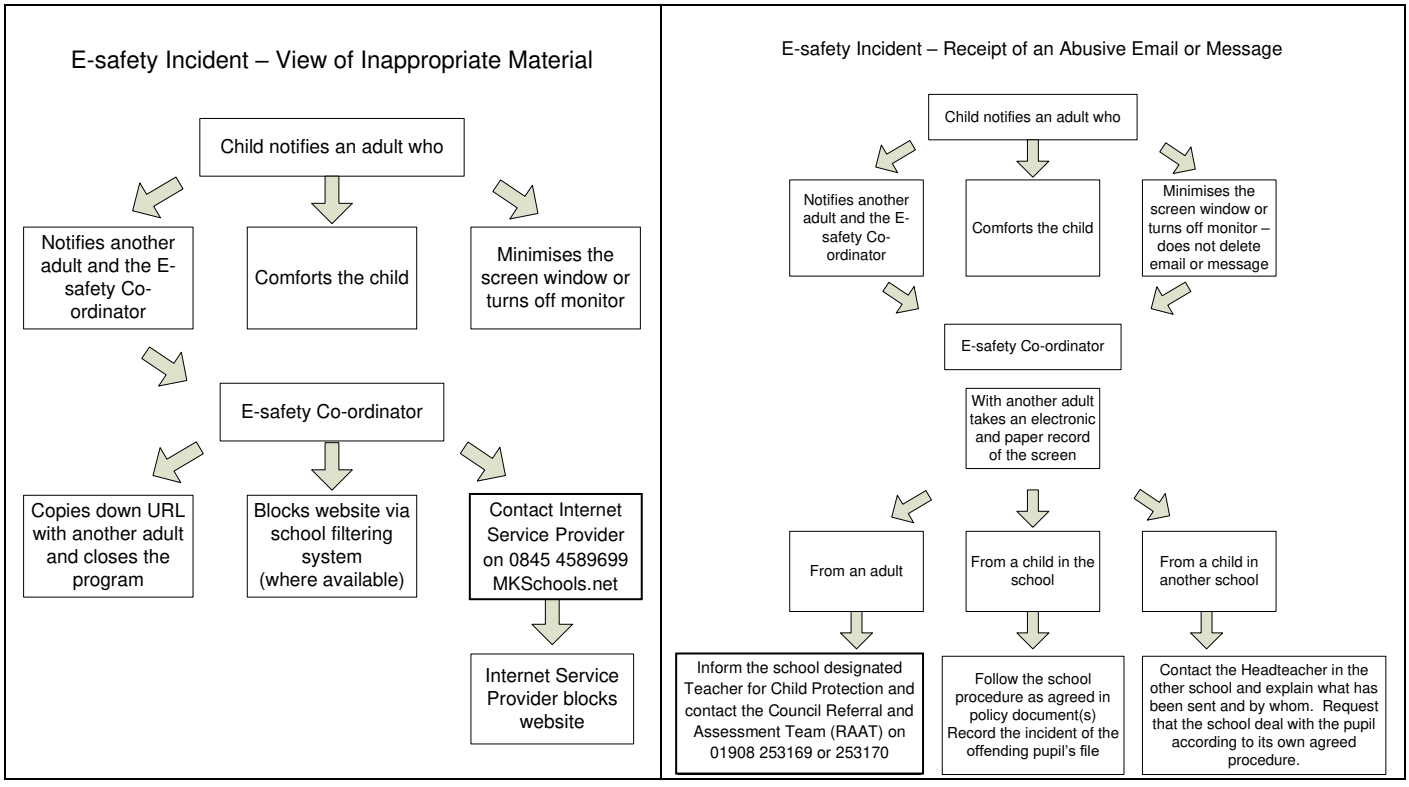
(c) Online Safety education programme

Children and staff are informed about issues and potential risks of using the Internet and related technologies so they are able to recognise when they might be in danger and take appropriate measures to protect themselves. If there are any issues the children can report them to their teacher, Learning Mentor or Pastoral Manager.

All of these elements should be addressed with all stakeholders, staff, children and young people plus parents/carers and governors, to take account of emerging technologies and changing local circumstances.

Dealing with Online Safety incidents

In most cases, the misuse of ICT is not serious and can be dealt with within school. The following diagrams illustrate actions that a school might take for two specific types of incident.



Appendix 1 Online Safety Incident Report Form

Online Safety Incident Report

Incident No:

Date of Incident:	Location of Incident:

Name of person who discovered / identified incident:

Brief description of incident
Brief description of any action taken at time of discovery

Comments / Notes

Date form sent to Online Safety Co-ordinator	Signature

Appendix 2 Summary of Online Safety Incident Log

This log, available as an Excel file, is provided as a basis for schools to use and adapt as required.

Incident Number
Date
Time
Nature of incident
Description of incident
Identified by
Pupil(s) involved
Staff involved
Action taken and by whom
Information recorded / secured
Hardware ID secured?
Online Safety Co-ordinator informed (by whom)
School Child Protection Officer informed (date+time) (by whom)
Council Child Protection Officer informed (name+date+time) (by whom)
Parents/Carers informed (date+time) (by whom)